Harmonizing People, Processes, and Technology for Robust Cybersecurity

D7.1 Beneficiary Information Package, Evaluation Metrics & Analysis Documentation, Beneficiary Financial Handbook v1

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D7.1 Beneficiary Information Package, Evaluation Metrics & Analysis Documentation, Beneficiary Financial Handbook v1		
Work Package	WP7 CYberSynchrony Financial Support to Third Parties		
Contractual due date	28/02/2026	**Actual submission date**	27/02/2026
Type	Report	**Dissemination Level**	Public
Lead Beneficiary	MAGGIOLI SPA (MAG)		
Responsible Author	Panos Papastergiou (MAG)		
Contributions from	N/A		

Funded by the European Union

ECCC

Funded by the European Union under Grant Agreement no. 101158555 and supported by the European Cybersecurity Competence Centre (ECCC). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	20.12.2025	Initial Deliverable structure	Panos Papastergiou (MAG)
0.2	20.01.2026	1st draft ready	Panos Papastergiou (MAG)
0.3	02.02.2026	2nd version ready, future actions were added; a refined template of the questionnaire was produced	Panos Papastergiou (MAG)
0.4	10.02.2026	Final draft ready for internal review	Panos Papastergiou (MAG)
0.5	13.02.2026	Internal review 1	George Karavokiros (BYTE)
0.6	18.02.2026	Internal review 2	Vasileios Roussakis (KETYAK)
0.7	19.02.2026	Final draft addressing comments from internal review	Panos Papastergiou (MAG)
0.8	20.02.2026	Initial QA review	Eleni Keliri (eBOS)
0.9	24.02.2026	100% of the deliverable ready for QA	Panos Papastergiou (MAG)
1.0	27.02.2026	Final version ready for submission	Violeta Vasileva (MAG)

Disclaimer

The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

1 Executive Summary 8
2 Introduction 9
2.1 WP7 Objectives and Tasks 7.1–7.4 9
2.2 Mapping CYberSynchrony Outputs 10
2.3 Linkage to other project outputs 12
2.4 Purpose and Scope of D7.1 13
2.4.1 Purpose 13
2.4.2 Scope 13
2.5 Deliverable Structure 14
3 CYberSynchrony FSTP Scheme Overview 15
3.1 End-to-end FSTP high-level workflow (from call publication to final payment) 15
3.2 Roles and Responsibilities (OCMT, Beneficiaries, External Evaluators) 16
3.2.1 Open Call Management Team - responsibilities 16
3.2.2 Beneficiaries' responsibilities 17
3.2.3 External evaluators' responsibilities 17
4 Beneficiaries and external evaluators information package – Overview 18
4.1 Objectives of the Beneficiary Information Package 18
4.2 Components and logic: Beneficiary Information Package, Beneficiary Financial Handbook and External Evaluator Package 18
4.2.1 Beneficiary Information Package 18
4.2.2 External evaluator package 19
5 Applicants' Information Package – Supporting Documentation 21
5.1 Open Call Guidelines for Applicants – role and scope 21
5.2 Proposal Technical Template – structure and required sections 21
5.3 FAQ – clarification of common issues 22
5.4 Consistency across supporting documents and online material 22
6 Applicants' Legal Documentation (Beneficiaries – Open calls) 24
6.1 Sub-grant agreements (single entity and consortium) 24
6.2 Declarations of Honour for different beneficiary types 24
6.3 SME Self-Declaration 24
6.4 Bank account information template 25
6.5 Declaration of Honour – consortium agreement 25
7 External Evaluators' Package 26
7.1 Information for external evaluators in the Open Call Guidelines 26
7.2 Required profile, expertise and workload expectations 26
7.3 Legal documentation for external evaluators 27
7.4 Assignment principles and allocation of proposals to evaluators 27
7.5 Ranking the external evaluators based on their experience and expertise 28
7.5.1 Tie-breaking rules for external evaluators 29
8 Evaluation Metrics & Analysis Documentation 30
8.1 Evaluation principles and governance 30
8.2 Proposal evaluation criteria and weights 30
8.2.1 Relevance and Excellence 30
8.2.2 Methodological Soundness 30
8.2.3 Ambition and Impact 30
8.2.4 Implementation / Team Skills and Expertise 31
8.3 Scoring scale, thresholds and tie-breaking rules 31
8.4 Evaluation forms and Evaluation Summary Reports (ESR) 31

© CYberSynchorny, 2026

8.5 Record-keeping and traceability 32
9 Beneficiary Financial Handbook 33
9.1 Lump-sum funding model and overall budget caps 33
9.2 Payment schedule (prefinancing, interim and final payments) 33
9.3 Monitoring procedures and interaction with CYberSynchrony technical partners 34
9.4 Management of deviations, underperformance and possible reduction/termination of support 35
9.5 Record-keeping, checks, audits and ex-post controls 35
9.6 Contact points and helpdesk 36
10 Future actions for D7.3 37
11 Conclusions 38
12 References 39
Annex I – Legal documentation for external evaluators 40
Annex II – Legal documentation for beneficiaries (FSTP) 41
Annex III – Supporting documentation for Open Call beneficiaries and external evaluators 42

List of Figures

Figure 1. Schematic on the Open Calls procedure 16

List of Tables

Table 1: WP7 Task descriptions 9
Table 2: Adherence to CYberSynchrony's GA 10
Table 3: Links to other Project Outputs/Work 12
Table 4: Components of the scope of D7.1 13
Table 5: Beneficiary information package: Legal Documentation 19
Table 6: Beneficiary information package: Supporting documentation 19
Table 7: External Evaluator package: Legal and supporting documentation 20
Table 8: YouTube videos on how to use the platform and apply as beneficiary or external evaluator 22
Table 9: Allocation approach of proposals to evaluators and ESR procedure 27
Table 10: Evaluation criteria for external evaluators 28
Table 11: Key financial parameters relevant to beneficiaries 33
Table 12: Standard payment schedule for CYberSynchrony sub-grants 34

© CYberSynchorny, 2026

Acronyms and abbreviations

Acronyms and terms	Description
AI	Artificial Intelligence
AI/ML	Artificial Intelligence / Machine Learning
API	Application Programming Interface
ASA	Attack Surface Assessment
ATT&CK	MITRE ATT&CK – Adversarial Tactics, Techniques and Common Knowledge framework
BYTE	Byte Computer: CYberSynchrony consortium partner (member of the OCMT)
CERT	Computer Emergency Response Team
CET	Central European Time (server time used for submission deadlines)
CI/CD	Continuous Integration / Continuous Deployment (automated software build, test and release pipeline)
CSIRT	Computer Security Incident Response Team
CSPA	Cyber Security Posture Assessment (dashboard for assessing organisational maturity and compliance posture)
CV	Curriculum Vitae
CVE	Common Vulnerabilities and Exposures (public catalogue of known security vulnerabilities)
CWE	Common Weakness Enumeration (classification of common software and hardware weaknesses)
CYberSynchrony	Project acronym: “Harmonizing People, Processes, and Technology for Robust Cybersecurity”
DCO	Defensive Cyber Operations (response playbooks for structured incident handling)
DEP	Digital Europe Programme
DoH	Declaration of Honour
EC	European Commission
ECS	Elastic Common Schema
EEA	European Economic Area
ESR	Evaluation Summary Report
EU	European Union
EUROPASS	Standardised European CV format (Europass CV)
EVE	Extensible Event Format
FAQ	Frequently Asked Questions
FP	Focal Point: CYberSynchrony consortium partner (member of the OCMT)
FSTP	Financial Support to Third Parties

© CYberSynchorny, 2026

GA	Grant Agreement for the CYberSynchrony project
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HRM	Human Risk Management (behavioural and awareness assessment of users)
HTTPS	Hypertext Transfer Protocol Secure
HTTPS/TLS	HTTPS over Transport Layer Security (encrypted web communication protocol)
IBAN	International Bank Account Number
IANUS	IANUS Technologies: CYberSynchrony consortium partner (member of the OCMT)
IDS	Intrusion Detection System
ISO	International Organization for Standardization
JWT	JSON Web Token (token format for API authentication and authorisation)
KPI	Key Performance Indicator
MAG	Maggioli SPA: (CYberSynchrony coordinator, WP7 leader and member of the OCMT)
MISP	Malware Information Sharing Platform
MITRE	MITRE Corporation
MS	Member State (of the European Union/EEA)
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)
OCMT	Open Call Management Team
OLAF	European Anti-Fraud Office
PC	Project Coordinator
PIC	Participant Identification Code
PTA	Purple Team Assessment
REST	Representational State Transfer (architectural style for web APIs)
SBS	Security Breach Simulation (controlled simulation of breach and ransomware scenarios)
SHA-256	Secure Hash Algorithm 256-bit (cryptographic hash function)
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprise
SOC	Security Operations Centre
STIX	Structured Threat Information eXpression
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAXII	Trusted Automated eXchange of Indicator Information
TRL	Technology Readiness Level
TRUST	Trustilio: CYberSynchrony consortium partner (technical partner and member of the OCMT)

© CYberSynchorny, 2026

UEBA	User and Entity Behaviour Analytics
URL	Uniform Resource Locator
VAT	Value Added Tax
WP	Work Package
WP7	Work Package 7 – CYberSynchrony Financial Support to Third Parties

© CYberSynchorny, 2026

1 Executive Summary

D7.1 establishes the complete framework for designing and operating the CYberSynchrony Financial Support to Third Parties (FSTP) scheme, in line with the Grant Agreement and the objectives of WP7. It consolidates, in a single reference document, the Beneficiary Information Package (Open Call Guidelines, Proposal Technical Template, FAQ), the full set of legal instruments for beneficiaries and external evaluators, the evaluation metrics and documentation, and the Beneficiary Financial Handbook describing the lump-sum model, payment schedule and monitoring arrangements. The deliverable first situates the FSTP scheme within the overall CYberSynchrony governance, describing the end-to-end workflow from call publication, outreach and application submission through eligibility checks, external evaluation, selection and contracting, to implementation, monitoring, payments and post-project feedback. It then details the information and legal packages for open call applicants and evaluators, clarifying the role of each document and fixing the exact templates in Annex I–III to ensure transparency and traceability of what is communicated externally.

The evaluation framework is fully specified, including the evaluation criteria, the scoring scale, thresholds, tie-breaking rules, and the principles for assigning proposals to evaluators and consolidating scores into Evaluation Summary Reports. The Beneficiary Financial Handbook defines the lump-sum funding model for the 8-month sub-projects (three instalments linked to defined milestones and reports), the associated reporting obligations, and the monitoring procedures and deviation-management logic that connect technical progress with payment decisions. At M21, the dedicated submission platform for both applicants and evaluators have been configured and tested, the documentation and rules described in D7.1 are publication-ready, and the open calls can be run using this framework. Lists of funded projects, empirical analysis of applicants' performance against the criteria and beneficiary feedback on the process will be provided in the subsequent WP7 deliverables (D7.2, D7.3 and D7.4), which will build on D7.1 by documenting the practical implementation and fine-tuning of the FSTP scheme.

© CYberSynchorny, 2026

2 Introduction

2.1 WP7 Objectives and Tasks 7.1–7.4

WP7, "CYberSynchrony Financial Support to Third Parties", designs and runs the sub-granting scheme in a compliant, transparent and impact-oriented manner over the whole lifecycle of the open calls. According to the Grant Agreement, its objectives are:

(1) to apply the established "financial support for third parties" methodology while ensuring compliance, transparency and maximum impact.

(2) to streamline all processes from application to fund disbursement, so that beneficiaries meet the eligibility and quality criteria and use the funds appropriately; and,

(3) to collect, review and act on feedback from beneficiaries in order to refine and enhance the methodology for any future cycles.

These objectives form the reference frame for all four Wp7 tasks (Table 1), and D7.1 focuses on the concrete documentation and rule set needed to implement T7.1 and T7.3. More information regarding the interaction of all tasks and deliverables linked to the GA are given in the Sections 2.2 and 2.3.

Table 1: WP7 Task descriptions

Task no	Task title	Task description
7.1	Beneficiary Outreach & Application Collection	covers the design and deployment of the awareness and outreach campaign, as well as the preparation and dissemination of clear application forms and guidelines so that potential beneficiaries can understand the calls and submit complete proposals.
7.2	Evaluation and Beneficiary Selection	defines how the collected applications will be assessed by a specialised review committee based on pre-established criteria, with the aim of a transparent, criteria-driven selection of those proposals that best fit the CYberSynchrony objectives
7.3	Fund Distribution and Monitoring	governs the disbursement of funds under predefined procedures and the monitoring mechanisms used to ensure that funds are used as intended and that beneficiaries progress towards their milestones in line with the Grant Agreement
7.4	Feedback Collection & Methodology Refinement	focuses on systematically gathering post-fund-disbursement feedback from beneficiaries and using it to adjust and improve the FSTP methodology over time. Within this structure, D7.1 provides the integrated information package, evaluation framework and financial handbook that implement the framework for Tasks 7.1–7.3 and create the baseline that Task 7.4 and its deliverables (D7.2 and D7.4) will later assess and refine.

© CYberSynchorny, 2026

2.2 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony's Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, in respect to their outputs and work to be performed (Table 2).

Table 2: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D7.1	Beneficiary Information Package, Evaluation Metrics & Analysis Documentation, Beneficiary Financial Handbook v1	Chapters 3, 4, 5, 6, 7, 8, 9, 10	D7.1 translates the WP7 FSTP-related commitments into a concrete, publication-ready framework. Chapters 3 and 4 describe the overall FSTP workflow and the logic of the Beneficiary Information Package and External Evaluator Package. Chapters 5, 6 and 7 document all supporting and legal documentation for beneficiaries and evaluators, corresponding to the "application forms, guidelines, FAQ and other relevant information" requested in the GA. Chapter 8 specifies the proposal evaluation criteria, scoring rules and tie-breaking, covering the "criteria used to evaluate the applicants, including the weight of each metric". Chapter 9 provides the Beneficiary Financial Handbook, detailing the lump-sum model, payment schedule, reporting requirements, monitoring procedures and deviation management. Chapter 10 summarises implementation status and remaining actions towards D7.3, which will complete the GA requirement for an analytical summary of applicants' performance once evaluations and sub-grant implementation have taken place.
TASKS			
Task number	**Task Title**	**Relevant Chapter No And Section**	**Brief outline how the GA task requirements are addressed**
7.1	Beneficiary Outreach & Application Collection	Chapters 3.1, 4, 5, 6, 7, 9.7	Task 7.1 requires CYberSynchrony to design and implement the open call process, prepare clear application forms and guidelines and ensure that potential beneficiaries can access and submit proposals efficiently. Chapter 3.1 presents the end-to-end FSTP workflow from call publication to final payment, including the submission platform. Chapters 4, 5 and 6 define the Beneficiary

© CYberSynchorny, 2026

			Information Package and all legal and supporting documentation that applicants must use (guidelines, proposal template, FAQ, declarations, SME form, bank form, sub-grant templates). Chapter 7 explains the information made available to external evaluators, which is part of the overall outreach to expert applicants. Chapter 9.7 sets out the contact points and helpdesk, completing the support structure for outreach and application collection. Together, these chapters show how D7.1 fulfils the Task 7.1 commitments on documentation, clarity and process, while the actual outreach campaign and collection of proposals are implemented operationally during the open call periods.
7.2	Evaluation and Beneficiary Selection	Chapters 3.1, 7, 8, 9.5	Task 7.2 requires a transparent evaluation and selection process based on pre-established criteria and independent external experts. Chapter 3.1 situates evaluation within the global FSTP workflow. Chapter 7 defines the External Evaluators' Package, including the call for evaluators, required profiles and legal framework; this underpins the "specialised review committee" foreseen in the GA. Chapter 8 sets out the four evaluation criteria, scoring scale, thresholds, tie-breaking rules, evaluator forms and record-keeping arrangements, directly operationalising the GA requirement for criteria and analysis documentation. Chapter 9.5 describes how deviations and underperformance may affect funding decisions, linking evaluation results with selection and possible reduction or termination of support. D7.1 therefore defines the rules, documentation and governance for Task 7.2; the concrete ranked lists and selection outcomes will be reported in D7.3 once the evaluations have been completed.
7.3	Fund Distribution and Monitoring	Chapters 3.1, 6.4, 9 (all subsections), 10	Task 7.3 focuses on disbursing funds under predefined procedures and monitoring that funds are used as intended, with progress towards milestones aligned with CYberSynchrony's objectives. Chapter 3.1 shows where contracting, payments and monitoring sit in the overall FSTP lifecycle. Chapter 6.4 describes the bank account information template required to execute payments. Chapter 9 defines the Beneficiary Financial Handbook: the lump-sum model and budget caps (9.1), the three-instalment payment

© CYberSynchorny, 2026

			schedule (9.2), reporting obligations and key milestones including the M4 interim check (9.3), monitoring procedures and interaction with technical partners (9.4), management of deviations and potential reduction or termination of support (9.5), and checks, audits and ex-post controls (9.6). Chapter 10 summarises what has been implemented at M21 and what will be evidenced in D7.3. These elements together demonstrate how D7.1 satisfies the Task 7.3 commitments on fund distribution rules and monitoring mechanisms.

2.3 Linkage to other project outputs

D7.1 is related to other project outputs, especially the CYberSynchrony modules, since these modules will be used by the beneficiaries (FSTP) in order to integrate them into their solutions (Table 3).

Table 3: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP3	T3.1–T3.4	D3.1, D3.2	WP3 develops the threat-intelligence platforms, unalterable forensic techniques, personalised risk assessment tools and dynamic risk parameter refinement that FSTP projects are expected to integrate, extend or complement. These technical capabilities are explicitly referenced in the Open Call guidelines as the core CYberSynchrony services with which funded solutions must interoperate.
WP4	T4.1–T4.4	D4.1, D4.2	WP4 provides the SIEM and traffic-analysis deployment, UEBA systems, automated incident-response playbooks and updated cyber risk/vulnerability database that define the monitoring and response environment into which sub-granted solutions will plug. The open call application and evaluation templates require applicants to position their solutions within this WP4 monitoring/response stack.
WP5	T5.1–T5.3	D5.1, D5.2	WP5 delivers the secure cross-border data-exchange platform and evidence-integrity mechanisms that govern how incident, threat and log data are shared and preserved. The sub-granting scheme uses these WP5 outputs as the reference architecture for data exchange and chain-of-custody, and applicants must show how their solutions align with or build on these platforms.

© CYberSynchorny, 2026

WP7	T7.2, T7.3, T7.4	D7.2, D7.3, D7.4	Within WP7, D7.1 provides the baseline information package, evaluation metrics and financial handbook that are then used by T7.2 for evaluation and selection (D7.2/D7.4) and by T7.3 for fund distribution and monitoring (D7.3). Thus, later WP7 outputs directly depend on and reuse the procedures, criteria and documentation defined in D7.1.

2.4 Purpose and Scope of D7.1

2.4.1 Purpose

The purpose of D7.1 is to provide a single reference package that enables a transparent and manageable Financial Support to Third Parties (FSTP) process for all CYberSynchrony open calls. It consolidates the information, rules and tools that applicants (beneficiaries[1] and external evaluators) need to understand the sub-granting scheme, prepare and assess proposals in line with the Grant Agreement, and implement funded projects under a clearly defined lump-sum funding and monitoring framework. D7.1 directly supports WP7 Objectives 1 and 2 by setting out how applications will be collected and evaluated and how funds will be disbursed and monitored, and it serves as the baseline that will later be refined in light of beneficiary feedback (D7.2 and D7.4) and actual implementation experience.

2.4.2 Scope

The scope of D7.1 covers three main components (Table 4):

Table 4: Components of the scope of D7.1

Component no	Title of component	Description of component
1	Beneficiary Information Package	documents the Beneficiary Information Package, namely the legal documentation and supporting material for both FSTP applicants and external evaluators, including the open call guidelines, proposal template, FAQ and the associated contractual and declaration templates, together with their intended use
2	Evaluation metrics, evaluation criteria, assigning proposal methodology	describes the evaluation metrics and related documentation, detailing the evaluation criteria and their weights, scoring scales and thresholds, and the principles for composing evaluation panels and assigning proposals to external experts in a way that is fair and traceable
3	Beneficiary Financial Handbook, monitoring methodology	provides the Beneficiary Financial Handbook, explaining the lump-sum model adopted, the payment schedule and milestones, the required technical and financial reporting, and the basic monitoring and compliance checks to be applied during implementation

[1] By beneficiaries, we mean the open call applicants (FSTP)

© CYberSynchorny, 2026

D7.1 focuses on defining these frameworks and documents; the lists of funded projects and the analysis of their performance and experience will be reported in subsequent versions (D7.2, D7.3 and D7.4).

2.5 Deliverable Structure

Chapter 1 – Executive Summary provides a concise overview of the purpose, main content, and key conclusions of the deliverable.

Chapter 2 – Introduction recalls the objectives and tasks of WP7, maps D7.1 to the Grant Agreement commitments and related project outputs, and clarifies the specific purpose and scope of this deliverable.

Chapter 3 – CYberSynchrony FSTP Scheme Overview describes the end-to-end FSTP workflow from call publication to final payment and defines the roles and responsibilities of the OCMT, beneficiaries and external evaluators.

Chapter 4 – Beneficiaries and external evaluators information package – Overview explains the objectives and overall logic of the Beneficiary Information Package, the Beneficiary Financial Handbook and the External Evaluator Package.

Chapter 5 – Applicants' Information Package – Supporting Documentation details the supporting documentation for applicants (Open Call Guidelines, Proposal Technical Template and FAQ) and how these documents work together and with the online material.

Chapter 6 – Applicants' Legal Documentation (Beneficiaries – Open calls) presents the legal documentation required from beneficiaries, including sub-grant agreement templates, Declarations of Honour, SME Self-Declaration, bank information form and consortium agreement declaration.

Chapter 7 – External Evaluators' Package sets out the information made available to external evaluators, the required profile and workload expectations, the legal documentation to be signed, and the principles for assigning and ranking evaluators, including tie-breaking rules.

Chapter 8 – Evaluation Metrics & Analysis Documentation defines the proposal evaluation principles, criteria and weights, the scoring scale, thresholds and tie-breaking rules, as well as the evaluation forms, Evaluation Summary Reports and record-keeping arrangements.

Chapter 9 – Beneficiary Financial Handbook describes the lump-sum funding model, budget caps, payment schedule, reporting and monitoring procedures, management of deviations, checks and audits, and the main contact and helpdesk channels for beneficiaries.

Chapter 10 – Future actions for D7.3 summarises the implementation status at M21 and lists the elements that will be completed and evidenced in the updated version of this deliverable (D7.3 – M22).

Chapter 11 – Conclusions summarises the overall contribution of D7.1 to the implementation of WP7 and indicates how subsequent WP7 deliverables (D7.2, D7.3 and D7.4) will build on the framework defined here.

© CYberSynchorny, 2026

3 CYberSynchrony FSTP Scheme Overview

3.1 End-to-end FSTP high-level workflow (from call publication to final payment)

This section presents the high-level workflow of the FSTP process, whilst more information and details will be provided in the following sections of this document.

The CYberSynchrony FSTP scheme follows a clear sequence that begins with the publication of the three open calls and ends with the final payment and feedback from funded sub-projects. The above procedure is schematically shown in Figure 1.

Each open call is announced together with all supporting material and the link to the dedicated submission platform which is the same for all three open calls. From that point, potential applicants consult the open call guidelines, verify their eligibility, and prepare their proposal using the mandatory proposal template and the appropriate legal declarations (Declarations of Honour, SME Self-Declaration, bank information as well as consortium agreement in case of consortia). Open call proposals and applications from external evaluators are submitted exclusively through the dedicated CYberSynchrony submission platform, which handles user registration, document upload and the official server-time stamping of submissions and applications.

Once the submission deadline has passed, all complete and eligible proposals move into the evaluation phase. Each proposal is assigned to two external evaluators, who apply the agreed five evaluation criteria on a 0–5 scale and provide narrative justifications. Their individual assessments are consolidated into a final score and an Evaluation Summary Report (ESR), which supports the generation of ranked lists, tie-breaking decisions, reserve lists and the preparation of notification letters. On this basis, the Open Call Management Team (OCMT) confirms which proposals are selected for funding, which are placed on the reserve list and which are rejected, in line with the rules described in the guidelines and the evaluation framework that D7.1 documents.

For the selected proposals, the next step is the contracting phase. Beneficiaries sign the appropriate sub-grant agreement (single entity or consortium) and, where relevant, the consortium agreement, together with the required Declarations of Honour. These documents formalise the scope, duration, lump-sum amount, internal distribution within consortia, and the payment and reporting obligations. Once contracting is completed, the sub-projects start and the first pre-financing instalment is paid within the defined timeframe. During implementation, beneficiaries carry out their 8-month work plan under the monitoring arrangements set out in the guidelines for applicants and the Beneficiary Financial Handbook. The lump-sum is structured in three payments: an initial pre-financing at project start, an interim payment linked to successful completion and validation of intermediate deliverables and reporting at M4, and a final payment after project end, once all remaining deliverables have been accepted. Monitoring and verification are performed jointly by the OCMT using agreed checklists and reporting templates. After the sub-projects completion, the beneficiaries will be invited to complete the D7.2 feedback questionnaire, which captures their overall experience with this full workflow and provides the evidence base for later refinement of the FSTP methodology in D7.4.

© CYberSynchorny, 2026

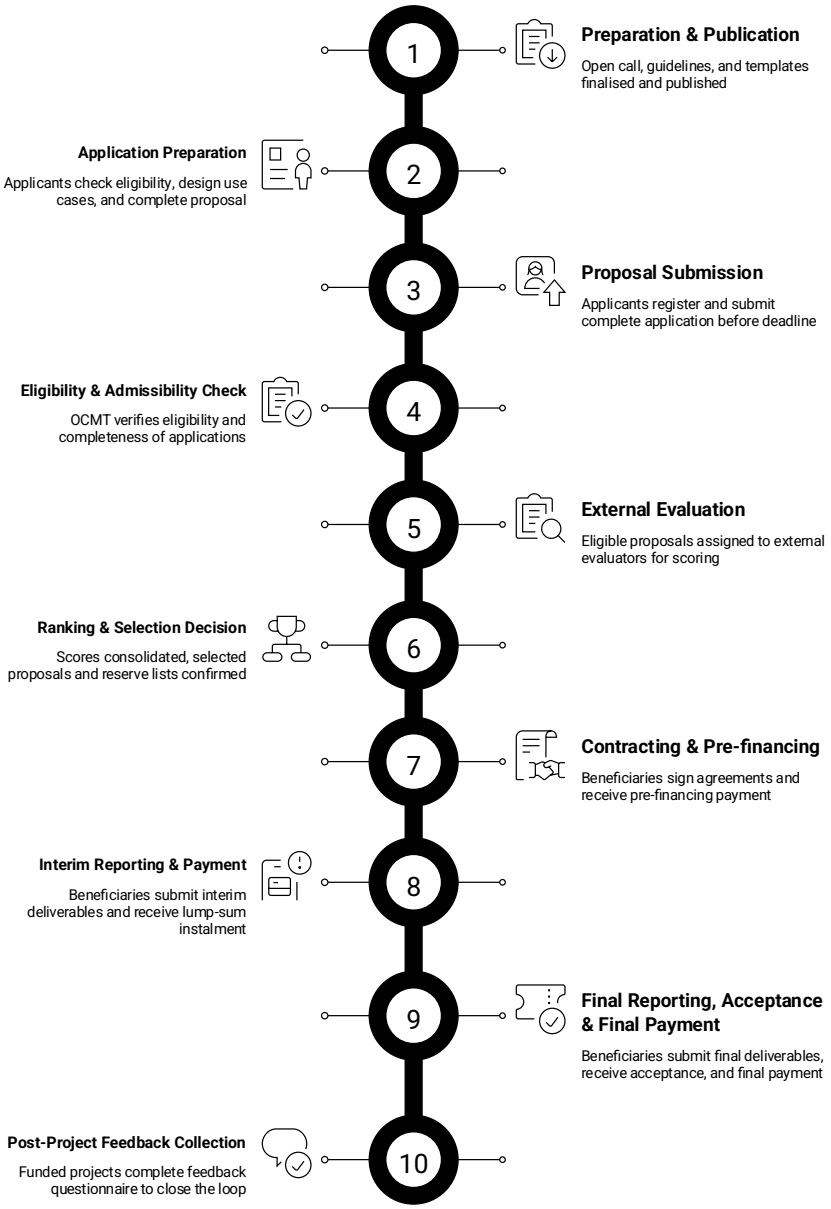

Figure 1. Schematic on the Open Calls procedure

3.2 Roles and Responsibilities (OCMT, Beneficiaries, External Evaluators)

The FSTP scheme in CYberSynchrony is implemented through a clearly defined division of roles between the Open Call Management Team (OCMT), the beneficiaries, and the external evaluators.

3.2.1 Open Call Management Team - responsibilities

3.2.1.1 Managerial tasks

The OCMT is responsible for the design and specifications of the Open Calls (FSTP), and supervising the implementation of the methodology phases as detailed in the grant agreement. This team is coordinated by MAG (CYberSynchrony's coordinator) and includes the technical representatives from the CYberSynchrony consortium (IANUS, FP, TRUST, BYTE). MAG will be responsible for the recruitment of the external evaluation experts to be involved in the evaluation process and the provision of content for the promotion of the Open

© CYberSynchorny, 2026

Calls implementation. MAG is also responsible for preparing and maintaining all legal and supporting documentation and operating the dedicated submission platform for both beneficiaries and external evaluators. It undertakes the eligibility checks, appoints and briefs the pool of external evaluators, oversees the application of the agreed four evaluation criteria (see section 8.2), and consolidates the individual assessments into a ranked list with the reserve and rejected proposals. MAG confirms the proposals selected for funding, coordinates the contracting phase (sub-grant and, where applicable, consortium agreements), and supervises the subsequent monitoring of lump-sum payments and milestones. The outputs of all above-mentioned tasks will be forwarded to the OCMT for final approval and for further amendments if necessary.

3.2.1.2 Technical support and mentoring

The OCMT will provide mentoring and implementation support to the beneficiaries once projects have been selected and contracted. Each technical partner will be responsible from 3 to 4 sub-grant projects and through monthly meetings will:

- validate the technical milestones
- check the technical deliverables associated with the interim and final lump-sum payments
- verify that the funded solutions progress as described and remain aligned with the project's cybersecurity objectives and integration requirements.

3.2.2 Beneficiaries' responsibilities

The beneficiaries are responsible first for preparing and submitting complete, eligible proposals using the official proposal template and all mandatory legal declarations and forms specified in the Open Call guidelines. If selected, they must sign the sub-grant agreement (and, where relevant, the consortium agreement and associated declarations of honour), implement the 8-month work plan as approved, and deliver the contractual outputs linked to the three lump-sum payments, including the interim report and deliverables at M4 and the final output package at project end. The beneficiaries must comply with the reporting and audit requirements set out in the sub-grant agreement and the Digital Europe Programme (DEP) rules [1], and cooperate with the OCMT during monitoring and verification. They are also expected to provide structured feedback on their experience with the FSTP process through the D7.2 questionnaire after final acceptance and payment (The completed questionnaires together with the analysis of the results will be included in D7.4).

3.2.3 External evaluators' responsibilities

The external evaluators are independent experts contracted by MAG to carry out the proposal evaluations. Under their contract and the associated Code of Conduct and Conflict of Interest declaration, they must read and analyse the call documentation and the proposals assigned to them, participate in the necessary briefings, and perform individual remote assessments using the agreed evaluation grid, providing both scores and narrative justifications. They are bound by strict obligations of independence, impartiality and confidentiality, and must systematically declare and avoid any conflict of interest for each proposal. Their evaluation reports (ESRs) constitute the primary technical basis on which the OCMT establishes the ranking, reserve list and funding decisions, but they are not involved in contracting or subsequent monitoring.

© CYberSynchorny, 2026

4 Beneficiaries and external evaluators information package – Overview

This package brings together all information, templates and legal instruments that applicants (beneficiaries and external evaluators) need in order to participate either in the CYberSynchrony open calls or as external evaluators in charge of reviewing the submitted Open Call proposals. It translates the high-level FSTP methodology defined in the Grant Agreement into a concrete, operational toolkit that can be used directly by the beneficiaries and external evaluators. This information is included in the "Open Call guidelines for applicants" (see Annex III - b).

From a process perspective, the Beneficiary Information Package supports three main phases: preparation and submission of proposals (Tasks 7.1 and 7.2), evaluation and selection (Task 7.2), and implementation and monitoring of the funded sub-grants (Task 7.3). For each phase it specifies what information is provided, which templates and legal documents must be used, how they are submitted and assessed, and what obligations beneficiaries and external evaluators must fulfil throughout all stages. D7.1 documents the structure and content of this package and points to the full, official versions of each document, which are attached as annexes to this deliverable.

4.1 Objectives of the Beneficiary Information Package

The primary objective of the Beneficiary Information Package is to ensure that the CYberSynchrony FSTP scheme is accessible, understandable and predictable for all participants. It must enable potential applicants to determine quickly whether they are eligible, what type of activities are supported, how to prepare a competitive proposal and which formalities are required. At the same time, it must give selected beneficiaries a clear view of their contractual, financial and reporting obligations over the 8-month implementation period, including the conditions for receiving each lump-sum instalment and the monitoring mechanisms that will be applied.

A second objective is to guarantee transparency and traceability of the evaluation and funding decisions. By publishing the evaluation criteria, their weightings and the main procedural rules (eligibility checks, scoring scale, thresholds, ranking and reserve lists), the package allows applicants to understand priorly how their proposals will be assessed and on which basis funding decisions are taken. Finally, the Beneficiary Information Package serves as a reference for external evaluators and for the OCMT itself, ensuring that all actors use the same definitions, criteria and templates throughout the FSTP lifecycle.

4.2 Components and logic: Beneficiary Information Package, Beneficiary Financial Handbook and External Evaluator Package

4.2.1 Beneficiary Information Package

The Beneficiary Information Package is structured into two components. The first component is the Legal Documentation Package, which targets organisations and individuals interested in applying to the CYberSynchrony open calls (Table 5).

© CYberSynchorny, 2026

Table 5: Beneficiary information package: Legal Documentation

Title of Legal Documentation	Annex (attached in this document)	Submission requirements
Declarations of Honour for each applicant type	Annex II – 2a, Annex II – 2b and Annex II – 2c	Upon submission of the proposals (only for SMEs, if other entities are included in the consortium, must be provided during the signing contract phase)
SME Self-Declaration	Annex II – 3	Upon submission of the proposals
bank information	Annex II - 4	must be provided during the signing contract phase
for consortia, the consortium agreement declaration	Annex II - 5	Upon submission of the proposals
sub-grant agreement templates	for single-entity Annex II - 6, or consortium (Annex II - 7)	must be provided during the signing contract phase
All documents are also available at https://cybersynchrony.eu/open-calls/		

The second component comprises the supporting documentation (Table 6). These documents describe the calls, eligibility and admissibility conditions, expected content of proposals and the formal requirements for a valid application.

Table 6: Beneficiary information package: Supporting documentation

Title of Supporting Document	Annex (attached in this document)	Submission requirements
Open Call guidelines for applicants *(including the Beneficiary Financial Handbook)*	Annex III - b	-
proposal technical template	Annex III - a	Upon submission of the proposals
the FAQ	Annex III - c	-
All documents are also available at https://cybersynchrony.eu/open-calls/		

Part of the second component is the Beneficiary Financial Handbook, which addresses applicants who become funded beneficiaries. It consolidates all information related to the lump-sum funding model, the payment schedule and conditions, the required technical and financial reporting, and the monitoring and verification procedures that will be applied by the OCMT. In practice, it draws on the sub-grant agreements, the financial and reporting clauses in the Open Call guidelines and the associated templates, and presents them in a beneficiary-oriented way, focusing on what has to be delivered, when and with which supporting evidence in order to receive each instalment.

4.2.2 External evaluator package

The External Evaluator package targets external experts interested in evaluating the proposals which will be submitted during the Open Call phase. Similarly, as the Beneficiary Information Package, this package comprises two components (the legal documentation and the supporting documentation) (Table 7). The evaluation framework and the role/responsibilities of the evaluators are provided in both components: parts of the Open Call guidelines define the evaluation framework and the role of evaluators, the expected profile

© CYberSynchorny, 2026

of experts and the obligations linked to independence, as well as the specific legal documents used to ensure confidentiality and conflict-of-interest. The successful evaluators will be invited to join an online meeting with the OCMT in order to clarify the procedure, how to use the submission platform to save their ESRs and to present the structure of the proposal template in order for them to mark the submitted open call proposals more efficiently.

Table 7: External Evaluator package: Legal and supporting documentation

Title of Legal Document	**Annex (attached in this document)**	**Submission requirements**
contract template *(includes also responsibilities and role)*	Annex I - A	must be provided during the signing contract phase
conflict of interest declaration	Annex I - B	
bank details form	Annex I - C	
All documents are also available at https://cybersynchrony.eu/open-calls/		
Title of Supporting Document	**Annex (attached in this document)**	**Source**
Open Call guidelines for applicants *(includes evaluation criteria)*	Annex III - b	All documents are also available at https://cybersynchrony.eu/open-calls/
Proposal template	Annex III - a	

More information regarding the Beneficiary and External Evaluator packages are given in Sections 5, 6, and 7.

© CYberSynchorny, 2026

5 Applicants' Information Package – Supporting Documentation

As defined in Section 4.2.1, the CYberSynchrony information package for applicants combines three core documents: the Open Call Guidelines for Applicants, the Proposal Technical Template and the Open Calls FAQ.

5.1 Open Call Guidelines for Applicants – role and scope

The Open Call Guidelines for Applicants (Annex III - b) is the primary reference document for both FSTP beneficiaries and external evaluators. They provide the overall context of CYberSynchrony, describe the three open calls under the FSTP scheme and explain how external tools, services and practices are expected to integrate with the CYberSynchrony framework.

From an operational point of view, the guidelines define all key parameters of the calls: the total FSTP budget (€3.55m), the maximum cumulative amount per third party (€200,000), the simultaneous launch of the three calls on the 1st January 2026 and the common submission deadline on the 1st March 2026 at 17:00 CET. They also describe the separate timeline for external evaluators (1 January 2026–15 February 2026).

The guidelines specify the mandatory use of the CYberSynchrony submission platform (https://cybersynchrony.grantplatform.com) for both proposal submissions and evaluator applications, including the rules on editing after initial submission and the use of server time (CET) as the only reference for deadlines. They define who is eligible to apply per open call, detail the proposal evaluation criteria, scoring scale, thresholds, ranking and tie-breaking rules, and describe the redress process available to applicants.

Further chapters set out the expected proposal structure, explain the intellectual property and results ownership regime, and codify conflict of interest rules separately for applicants and external evaluators.

The guidelines also summarise the sub-grant agreement framework and list which legal documents are mandatory at application, and which will be required at contracting, thereby acting as the narrative counterpart of the legal package presented in Section 4 of this deliverable.

The guidelines also describe the core CYberSynchrony modules and point beneficiaries to relevant public deliverables that contain essential technical and architectural information. This ensures that proposals can be aligned with the project's existing capabilities and integration expectations, and that the open calls effectively extend the CYberSynchrony ecosystem rather than duplicating or misaligning with it.

5.2 Proposal Technical Template – structure and required sections

The Proposal Technical Template is the mandatory format that all FSTP beneficiaries must use when preparing their submissions. It applies the guidance provided in the Open Call Guidelines into a concise, structured document that allows evaluators to apply the agreed criteria consistently. The template also enforces page limits and formatting rules, helping to keep proposals focused and comparable across the portfolio.

The template is organised into five main sections that correspond directly to the four evaluation criteria (Section 8.2) used in CYberSynchrony (Relevance and Excellence; Methodological Soundness; Ambition and Impact; Implementation; Team Skills and Expertise).

- **Section 1** collects the basic administrative and summary information about the proposal.
- **Section 2** focuses on Relevance and Excellence, asking applicants to justify alignment with the specific open call, the CYberSynchrony objectives and the targeted sectors.
- **Section 3** describes the technical approach and methodology, including how the proposed tools, services or practices will be designed, integrated and validated.

© CYberSynchorny, 2026

- **Section 4** focuses on Ambition and Impact, covering expected benefits for the targeted sectors, contribution to cybersecurity resilience and cross-border cooperation, and scalability beyond the project.
- **Section 5** addresses Implementation, including work plan, milestones, risk considerations and resources including budgeting.

5.3 FAQ – clarification of common issues

The CYberSynchrony Open Calls FAQ complements the Guidelines and Proposal Template by addressing recurring questions in a concise, accessible format. It is designed as a practical help tool rather than a normative document: it does not introduce new rules but clarifies how the existing ones should be interpreted in typical situations faced by applicants and external evaluators.

The FAQ explains the overall purpose of the three open calls, summarising their focus areas and how they relate to the NIS2 sectors [1] and cross-border cooperation ambitions of the project. It recaps the total budget and the €200,000 cap per third party and provides concrete clarifications on sectoral scope (for example, how proposals in sectors not explicitly listed in the call text can still be eligible if they fall within the NIS2 Directive [1] and are well-justified).

Several questions address key procedural aspects: the exact opening and closing dates of the calls, the use of the dedicated platform, the possibility to edit applications after submission, and the rule that only the platform server time (CET) is considered for deadline compliance. The FAQ also clarifies who can apply by country, consistent with Digital Europe Programme eligibility, and indicates where applicants and evaluators can find more detailed information on the project website and in the guidelines.

5.4 Consistency across supporting documents and online material

The three supporting documents are intentionally designed as a coherent package. The Guidelines set out the formal rules and parameters of the open calls, the Proposal Technical Template translates these rules into a standardised proposal structure aligned with the evaluation criteria, and the FAQ addresses common points of uncertainty without altering the underlying framework.

All three documents are made available through the CYberSynchrony Open Calls webpage, alongside additional material such as YouTube tutorials on how to use the submission platform (Table 8).

Table 8: YouTube videos on how to use the platform and apply as beneficiary or external evaluator

Description of video	YouTube link
Instructions on how to use the submission platform for beneficiaries (FSTP)	https://www.youtube.com/watch?v=pNcNGIle8Ic
Instructions on how to use the submission platform	https://www.youtube.com/watch?v=9JVI1LnEw4s
General promotional video for Open Calls	https://www.youtube.com/watch?v=eL7XQrh5csE

The design of D7.2 further reinforces this consistency: several questions in the feedback questionnaire explicitly ask beneficiaries to rate the clarity and usefulness of the Guidelines, the Proposal Template and the FAQ, as well as the description of eligibility rules, evaluation criteria and payment conditions.

This creates a closed loop between the information package described in the present section and the later methodological refinement work under Tasks 7.2 and 7.4, enabling CYberSynchrony to adjust these

© CYberSynchorny, 2026

documents in future iterations based on systematic beneficiary feedback while preserving alignment with the Grant Agreement and Digital Europe Programme requirements.

© CYberSynchorny, 2026

6 Applicants' Legal Documentation (Beneficiaries – Open calls)

6.1 Sub-grant agreements (single entity and consortium)

The core contractual instrument between CYberSynchrony and each funded sub-project is the sub-grant agreement, issued in two versions depending on whether the beneficiary applies as a single entity or as a consortium. Both versions translate the provisions of the CYberSynchrony Grant Agreement and the Digital Europe Programme (DEP) rules [1] into a sub-contractual framework that can be signed directly with third-party beneficiaries, covering the 8-month implementation period and the associated lump-sum funding.

Each sub-grant agreement formalises the scope of work to be carried out under the open call, the project duration, the total lump-sum amount awarded, the internal distribution of that amount in the case of consortia, and the beneficiaries' obligations regarding reporting, monitoring and verification. It specifies the milestones and deliverables that condition the release of each instalment and refers to the payment schedule and monitoring arrangements described in the Beneficiary Financial Handbook (section 4.2.1), thereby ensuring consistency between the narrative guidance and the legally binding clauses. The sub-grant agreements also clarify the relationship between beneficiaries and the CYberSynchrony consortium, including the role of the OCMT in monitoring progress and validating results before each payment.

6.2 Declarations of Honour for different beneficiary types

In addition to the sub-grant agreement, all beneficiaries are required to sign a Declaration of Honour (DoH) that reflects their legal nature and confirms that they meet the eligibility and non-exclusion conditions of the open calls as defined in the Open Call Guidelines for Applicants.

The individual and organisation-specific Declarations of Honour (Annex II - 2a, Annex II - 2b, Annex II - 2c) ensure that each applicant formally confirms the accuracy of the information submitted in the proposal and accompanying forms, acknowledges the conditions of the call, and commits to comply with the requirements set out in the CYberSynchrony open call documentation and the underlying DEP rules [1]. They allow the OCMT to verify, in a standardised way, that applicants fall within the permitted categories (e.g. SME, research organisation, public body, individual expert) and that no declared exclusion or incompatibility exists with respect to participation.

The "Open Call Declaration of Honour – consortium agreement" (Annex II - 5) complements the individual declarations in cases where two or three partners form a consortium. It confirms that the consortium partners have agreed on their internal roles, responsibilities and financial distribution, and that they collectively accept the terms of the open call and the sub-grant agreement to be signed with CYberSynchrony.

6.3 SME Self-Declaration

Because the CYberSynchrony scheme is centred on SMEs as coordinators of the funded projects, beneficiaries must provide structured evidence of their SME status. The SME Self-Declaration (Annex II - 3) requires applicants to supply the basic company data (such as identification details and size indicators) necessary for OCMT to verify that they qualify as an SME under the eligibility framework of the open calls and, by extension, the applicable DEP rules [1]. It is used together with the relevant Declaration of Honour (Annex II - 2c for SMEs and, where relevant, Annex II - 5 for consortia) to ensure that the designated coordinator legitimately fulfils the SME requirement set out in the guidelines and that any SME-specific provisions in the sub-grant agreement and payment modalities are applied only to eligible entities.

© CYberSynchorny, 2026

6.4 Bank account information template

To enable the correct and timely payment of sub-grants, successful applicants (beneficiaries and external evaluators) must provide complete and verifiable bank account details (Annex II - 4 and Annex I - C, respectively). The beneficiary template collects standardised information on the account holder and the bank (account name, address, contact person, IBAN/account number, SWIFT code, etc.), and requires either a bank stamp and signature of a bank representative or, alternatively, the attachment of a recent bank statement (not older than two months).

For external evaluators, the form has the same structure and purpose but is tailored to individual experts contracted by MAG under the external evaluator contract. In both cases, the use of standardised bank forms ensures that account data are captured in a consistent format across all beneficiaries and evaluators, reducing the risk of payment errors and facilitating compliance with the Digital Europe financial management requirements.

6.5 Declaration of Honour – consortium agreement

In cases where two or three entities apply as a consortium, the "Open call declaration of honour – consortium agreement" acts as a binding statement of their internal arrangements for the purposes of the CYberSynchrony open calls. The template is provided in Annex II – 5: "Open Call Declaration of Honour - consortium agreement". It records the identification of the lead beneficiary and the other consortium beneficiaries, confirms that they have agreed on their roles and budget shares, and designates the lead beneficiary as solely responsible for distributing the budget shares to the other partners. It also clarifies that the CYberSynchrony consortium bears no responsibility for any internal disputes among consortium beneficiaries, including those related to budget distribution or intellectual property.

The consortium Declaration of Honour further confirms that the consortium members have not submitted any other proposal under the same CYberSynchrony open call and that they collectively accept all rules explained in the Open Call Guidelines for Applicants, including the maximum cumulative €200,000 cap per applicant across all three open calls. It also incorporates the standard exclusion and non-conflict-of-interest clauses required under EU funding rules. By signing this document, all consortium partners formalise their mutual commitments before entering into the sub-grant agreement, thereby creating a clear link between the internal consortium arrangements and the external contractual relationship with CYberSynchrony.

© CYberSynchorny, 2026

7 External Evaluators' Package

The External Evaluators' Package specifies how experts can apply to join the CYberSynchrony evaluator pool, which rules govern their work, and which legal and administrative documents must be signed before they can be contracted and paid. The detailed list of all documentation in given in Section 4.2.2.

7.1 Information for external evaluators in the Open Call Guidelines

The Open Call Guidelines for Applicants (Annex III - b) include a dedicated section on external evaluators, which defines the application timeline, the submission channel, and the core principles (confidentiality, non-disclosure, independence and conflict-of-interest management) that apply to all evaluations.

The call for external evaluators opens on 1 January 2026 and closes on 15 February 2026 at 17:00 CET.

Applications must be submitted exclusively via the CYberSynchrony submission platform (https://cybersynchrony.grantplatform.com), where evaluators register, complete their profile and upload the requested information; applications submitted by email or any other means are not accepted.

Evaluators may edit their application after the initial submission, but no further changes are possible after the application deadline and the submission process is locked by the platform; the system's server time (CET) is the only reference for determining whether an application is received on time.

The Guidelines further state that all evaluations will be carried out under strict confidentiality and conflict-of-interest rules. Evaluators must treat all proposal information as strictly confidential, may not disclose proposal content, applicant identity, or other evaluators' opinions to third parties, and must not have been involved in the preparation of any proposal they assess or benefit from its acceptance or rejection.

Any potential conflict of interest must be declared immediately; if confirmed, the evaluator must withdraw from the assessment of the affected proposal(s).

The Guidelines thus provide the high-level framework that is then implemented in more detail through the evaluator contract and the dedicated Conflict of Interest form (Annex B).

7.2 Required profile, expertise and workload expectations

CYberSynchrony seeks external evaluators with strong expertise in cybersecurity and related regulatory and operational domains, in line with the nature of the three open calls and the project's emphasis on NIS2-relevant sectors [1]. As described in the call material and internal WP7 design, ideal evaluators should combine:

technical knowledge of cybersecurity tools, architectures and standards (e.g. threat intelligence platforms, orchestration and incident-response tools, secure communication and data-sharing mechanisms), familiarity with cross-border cybersecurity collaboration and regulatory frameworks (including NIS2-related requirements and data protection constraints), and experience in assessing complex, innovation-oriented projects, preferably including EU or national R&I or deployment programmes.

In addition, evaluators are expected to have strong analytical and drafting skills to score proposals against the five CYberSynchrony evaluation criteria and provide concise but substantive justifications for each criterion and the overall assessment. Their work is carried out remotely, based on the documentation provided via the platform and any briefing material prepared by OCMT, and must follow the evaluation grid and instructions set out in the Guidelines and internal evaluation handbook.

Workload expectations are defined by the number of proposals assigned to each expert and the standard fee per proposal. CYberSynchrony foresees a fee of €90 per evaluated proposal, corresponding to a

© CYberSynchorny, 2026

reference rate of €450 per working day for five proposals. A typical evaluation assignment will consist of batches of up to 10 proposals (2 working days) and the exact number of required experts will depend on the final volume of submissions and the need to balance workloads across the evaluator pool. All work must be completed within the evaluation period indicated on the project website, and evaluators are expected to respect the internal deadlines for submitting their individual assessments so that OCMT can consolidate scores and finalise rankings on time.

7.3 Legal documentation for external evaluators

The legal framework for engaging external evaluators is provided in Section 4.2.2. More details regarding each document is presented below:

The ***Contract for external evaluator*** (Annex I - A) sets out the subject of the contract, the tasks to be performed (reading and analysing proposals and call documentation, participating in briefings and meetings where required, and drafting and submitting evaluation reports), the working arrangements (remote work, planning and deadlines, maximum working days), the fee conditions, and the rights and obligations of both parties. It includes a Code of Conduct, which elaborates on impartiality, confidentiality and proper performance of the work, and a Declaration of Honour on exclusion criteria and absence of conflict of interest. Additional annexes cover the tax declaration and supplier registration sheet required by MAG, ensuring compliance with fiscal and procurement rules.

The ***Conflict of Interest form*** (Annex I - B) is a stand-alone declaration that applies the guidelines' principles on independence and confidentiality. Evaluators formally acknowledge the definition of conflict of interest, commit to informing OCMT of any situation that could compromise their impartiality, and agree to strict confidentiality obligations regarding proposal content, the evaluation process, other evaluators and the outcome of the work. They also undertake to return, erase or destroy all confidential documents after the end of the work and to refrain from communicating with applicants outside the formal channels.

The ***Bank details form*** (Annex I - C) collects the evaluator's bank account and contact information necessary for processing payments, including account holder data, IBAN or account number, SWIFT code and bank identification, together with a bank stamp or recent bank statement and the evaluator's signature. This form must be submitted alongside the signed contract and declarations to allow MAG to execute payments once the evaluator has completed the assigned work and submitted the required evaluation reports.

7.4 Assignment principles and allocation of proposals to evaluators

The allocation of proposals to the successful external evaluators is managed centrally by the OCMT to ensure independence, consistency and fairness across all three open calls. Once the submission deadline has passed and the eligibility checks have been completed, each eligible proposal is assigned to two external evaluators, in line with the Grant Agreement (Table 9).

Table 9: Allocation approach of proposals to evaluators and ESR procedure

Phase	Approach
Phase 1: Assign the proposals to evaluators	Each proposal will be evaluated by 2 external evaluator experts. The assignment will be done by the submission platform. This takes into consideration the following rule: Up to 10 proposals per evaluator (however, depending on the number of the successful Open Call applications, in comparison with the number of the successful

© CYberSynchorny, 2026

	evaluators, the maximum number of the assigned proposals may be higher to address the demand)
Phase 2: Individual ESRs	Each external evaluator will produce an ESR according to the evaluation criteria and scoring scale. In order a proposal to be eligible for funding, it must achieve a minimum score of 3 out of 5, in all evaluation criteria.
Phase 3: Consolidation of the results	MAG will consolidate the 2 ESRs into one, keeping all comments from both evaluators but using the average score for each evaluation criterion.
Phase 4: Consensus meetings (If required)	When the difference is more than 2 points in any of the evaluation criteria, both external evaluators must have a consensus meeting between them and agree on a final score for this criterion.

7.5 Ranking the external evaluators based on their experience and expertise

Based on the evaluators' profiles collected through the CYberSynchrony submission platform and the information provided in their applications, MAG in collaboration with the OCMT will rank the external evaluators.

Through their application, the external evaluators have to elaborate on the following 3 main areas:

1. Current Position and Organisation Name
2. Professional expertise and background
3. Previous Evaluation Experience

Apart from the above, it is mandatory for the external evaluators to upload their CV in a EUROPASS format for the OCMT to have the complete picture of their expertise. In addition, the applicants have to provide their LinkedIn account link.

MAG will then evaluate each external evaluator application based on the following 6 criteria (Table 10). Each criterion has a maximum score of from 15 to 20, and the maximum score that each evaluator can get is 100 at 5-point intervals. After this procedure is completed, the list of the evaluations of all applicants will be forwarded to the OCMT for the final check and approval.

Table 10: Evaluation criteria for external evaluators

Criterion	Maximum score
CR1: General Cybersecurity/computer science experience;	20
CR2: Expertise in cybersecurity technologies and frameworks (e.g., MISP, STIX/TAXII, ThreatConnect);	15
CR3: Experience evaluating complex cybersecurity proposals or projects;	20
CR4: Familiarity with automation, orchestration, and incident response tools;	15
CR5: Knowledge of cross-border cybersecurity collaboration, data privacy, and secure communication standards;	15
CR6: Strong analytical skills with the ability to assess both technical and strategic aspects of proposals.	15

© CYberSynchorny, 2026

7.5.1 Tie-breaking rules for external evaluators

Tie-breaking rules are applied only when they affect the final selection at the cut-off point. After scoring and ranking, the project selects the minimum number of evaluators needed to cover all proposals (based on the capacity rule – see Phase 1 - Table 9). If the last available place(s) fall within a group of evaluators with the same score, the tie-breaking rules are used only to decide which evaluator(s) from that equal-score group are included in the selected pool and which are kept as reserves. If there is no tie at the cut-off (e.g., all evaluators above the cut-off score are clearly within the required number, and the next score below is lower), no tie-breaking is performed because it does not change the selection outcome.

In case of tie-breaking, the following rules will be followed:

1. Higher CR3 (Evaluation experience score)
2. Higher CR2 (Expertise score)
3. Higher domain fit where it matters most for CYberSynchrony calls: compare (Q4 + Q5); higher sum wins (automation/orchestration/incident response + cross-border/privacy/security).
4. Higher CR6 (Analytical skills score)
5. If the above four rules are applied and there is still a tie, then the applications will be reassessed, but instead of using the 5-point interval point score, a 1-point interval score will be applied for all 6 evaluation criteria (Table 10) and then, the first-4 tie-breaking rules will be followed again if necessary.

© CYberSynchorny, 2026

8 Evaluation Metrics & Analysis Documentation

8.1 Evaluation principles and governance

The CYberSynchrony FSTP evaluation is governed by a set of principles that are explicitly described in the Open Call guidelines for applicants (Annex III - b) and implemented by the Open Call Management Team (OCMT) together with the external evaluators. Each complete and eligible proposal, after the eligibility checks described earlier in this deliverable, is assigned to two external evaluators from the pre-selected pool, following the methodology described in Section 7.4.

Evaluators assess the proposals remotely using a common evaluation grid and the four agreed criteria defined in the guidelines (see Section 8.2). They provide both numerical scores and concise narrative justifications, which together form the basis of the Evaluation Summary Report (ESR) that is later communicated to applicants.

The final scores and the tie-breaking rules described in Section 8.3, the OCMT compiles the ranked list of proposals, the reserve list and the list of rejected proposals. The OCMT then validates the outcome and issues the provisional list of successful applicants, which is communicated together with ESRs and information on the redress procedure. The redress mechanism, also governed by OCMT, is strictly limited to procedural and eligibility issues and does not reopen the technical or impact judgements of the experts.

8.2 Proposal evaluation criteria and weights

The evaluation framework uses four criteria, defined in Table 6 of the Open Call guidelines and applied identically across all three open calls. Each criterion is scored on a 0–5 scale and contributes equally to the overall score (maximum 5 points per criterion, overall maximum 20 points).

8.2.1 Relevance and Excellence

This criterion assesses how clearly the proposal defines its objectives and how well these align with the CYberSynchrony vision and the specific open call scope. The proposal must identify concrete cybersecurity vulnerabilities or challenges, explain the main goals of the work, and show a clear fit with the call's objectives and KPIs (for each open call: Open Call 1 – Section 2.1, Open Call 2 – Section 2.2, Open Call 3 – Section 2.3 of Annex III - b).

8.2.2 Methodological Soundness

Here the evaluators judge whether the proposal presents a coherent and technically credible approach for achieving its objectives. The methodology must describe the technical and operational steps, tools and frameworks to be used, the sequencing of activities, dependencies and validation strategy. The proposal must make explicit how it will interface with CYberSynchrony architecture and modules, so that evaluators can see not only what the team intends to do but how it will be implemented in practice.

8.2.3 Ambition and Impact

This criterion examines the ambition of the proposed work and the expected technical, operational and market-level impact. Evaluators check whether the results will contribute meaningfully to the objectives and KPIs defined for the corresponding open call, including improvements in cybersecurity resilience, regulatory readiness, cross-border collaboration and uptake of CYberSynchrony solutions. Proposals must articulate plausible, measurable outcomes rather than generic statements of benefit.

© CYberSynchorny, 2026

8.2.4 Implementation / Team Skills and Expertise

The fourth criterion combines the quality of the implementation plan with the adequacy of the team. The proposal must present a realistic and structured work plan (work packages, tasks, timeline for the 8-month duration, milestones and deliverables) that fits the lump-sum funding model, including risk identification and mitigation measures. At the same time, applicants must demonstrate that the team has the necessary technical, cybersecurity and regulatory expertise, particularly in the targeted NIS2 sectors [1], and that relevant prior experience is clearly described and linked to the proposed roles in the project. Inadequate justification of requested resources is explicitly penalised under this criterion (see Section 8.3).

Because each of the four criteria has a maximum of 5 points, they are effectively equally weighted in the total score. No additional numerical weighting factors are applied beyond this equal contribution.

8.3 Scoring scale, thresholds and tie-breaking rules

All four criteria are scored on a numeric scale from 0 to 5, with increments of 0.5 allowed. The overall maximum score for a proposal is therefore 20 points. The interpretation of scores follows the standard Digital Europe scheme: 0 = fail (criterion not addressed or assessment impossible), 1 = poor, 2 = fair, 3 = good, 4 = very good and 5 = excellent. A minimum threshold of 3/5 applies to each individual criterion; proposals falling below this threshold on any criterion are not eligible for selection, regardless of their total score. In particular, insufficient justification of costs and resources leads to a below-threshold score under the Implementation criterion.

After scoring, proposals are ranked by total score. In case of ties, the following sequence of tie-breaking rules is applied, exactly as specified in the Open Call guidelines:

- Priority is given to the proposal with the stronger innovation of the concept (Criterion 1 – Section 8.2.1).
- If still tied, priority goes to the proposal whose technology better fits the CYberSynchrony scope (Criterion 2 – Section 8.2.2).
- If still tied, priority goes to the proposal with higher impact and market potential (Criterion 3 – Section 8.2.3).
- If still tied, priority goes to the proposal with the lower funding request.
- If still tied, priority goes to the proposal with the higher number of female researchers in the team.
- If still tied, priority goes to the proposal that contributes more to increasing the CYberSynchrony footprint in Europe (e.g. by involving additional countries or under-represented regions).
- If proposals remain inseparable after all above-mentioned six rules, an additional evaluator from the external evaluators' pool is appointed to re-evaluate the tied applications and break the tie. A reserve list of the highest-ranked unfunded proposals is maintained to allow replacement in case any selected applicant withdraws or fails to meet contractual obligations.

8.4 Evaluation forms and Evaluation Summary Reports (ESR)

For each proposal assigned to them, external evaluators complete a structured online evaluation form on the CYberSynchrony submission platform. The form mirrors the four evaluation criteria defined in Section 8.2 and used across all three open calls. For every criterion, evaluators provide a numerical score on the 0–5 scale described in Section 8.3, together with a short, text-based justification that highlights the proposal's main strengths and weaknesses against that criterion.

Once both individual evaluations are submitted, the OCMT follows the approach described in Section 7.4 to consolidate the results into a single Evaluation Summary Report (ESR) for each proposal. The ESR presents,

© CYberSynchorny, 2026

in a single document, the final score, the breakdown by criterion, and the comments made by both evaluators. This consolidated ESR is the main technical input used by the OCMT to establish the ranked list, to differentiate between proposals around the funding threshold, and to populate the reserve list. The same ESR is communicated to applicants together with their result notification.

8.5 Record-keeping and traceability

All evaluation-related records are kept in a way that allows full traceability of the selection process from submission to final funding decision. The submission platform stores the complete history of each proposal, including submission time-stamps, eligibility checks, evaluator assignments, individual evaluation forms, consolidated ESRs, and the final ranking status (funded, reserve list, not funded). Access to these records is restricted to the OCMT, and is governed by CYberSynchrony's internal data protection and access-control procedures, in line with the Grant Agreement and applicable GDPR [1] obligations.

In addition to the electronic records, the OCMT keeps a structured archive of key decision documents, such as the final ranked lists approved for each open call, formal minutes or notes from OCMT meetings where borderline or exceptional cases were discussed, and any redress or complaint correspondence together with the related clarifications. Conflict-of-interest and confidentiality declarations signed by the external evaluators, as well as their contracts, are stored together with the evaluation records so that independence can be demonstrated at any later audit.

© CYberSynchorny, 2026

9 Beneficiary Financial Handbook

9.1 Lump-sum funding model and overall budget caps

The CYberSynchrony FSTP scheme provides financial support exclusively in the form of lump-sum grants. The awarded amount is not reimbursed on the basis of actual incurred costs; instead, each sub-grant is linked to a predefined set of outputs (deliverables and milestones), and payments are released only after these outputs have been successfully delivered and verified, as specified in the sub-grant agreement.

Across the three open calls, CYberSynchrony allocates a total FSTP budget of €3,550,000. A maximum of €200,000 may be awarded to any single third party across all open calls combined. Each third party may participate in only one proposal per call, and multiple participations in the same call result in the disqualification of all such proposals.

The open calls define funding ranges per call and consortium size, together with thematic caps for specific activity categories, ensuring a balanced distribution of resources and alignment with the strategic priorities of the project (infrastructure and operations, compliance and innovation, cross-border coordination). The exact lump-sum requested by each proposal must respect these ranges and caps, and becomes a fixed amount once the sub-grant agreement is signed.

Table 11 below summarises the key financial parameters relevant to beneficiaries.

Table 11: Key financial parameters relevant to beneficiaries

Parameter	Provision
Total FSTP budget	€3,550,000 across three open calls
Funding instrument	Lump-sum grants tied to output verification
Maximum funding per third party	€200,000 across all open calls combined
Project duration (per sub-grant)	8 months
Number of instalments	Three (prefinancing, interim, final)
Proposal limit per call	One proposal per third party; multiple participations lead to exclusion
Funding ranges and thematic caps	Defined per call and consortium size, with activity-specific caps (see Open Call Guidelines, Tables 2–4)

The detailed legal provisions that formalise the awarded lump-sum, internal distribution in consortia and associated obligations are laid down in the sub-grant agreement and related annexes (Annex II 6 and Annex II - 7), while the funding rules and caps are consolidated in the Open Call Guidelines (Annex III - b).

9.2 Payment schedule (prefinancing, interim and final payments)

The lump-sum awarded to each funded project is split into three instalments, each linked to specific contractual events and verifications defined in the sub-grant agreement and the approved proposal (Table 12).

© CYberSynchorny, 2026

Table 12: Standard payment schedule for CYberSynchrony sub-grants

Instalment	Share of total lump sum	Indicative timing*	Conditions for payment
Prefinancing	30%	Month 1, within one month after sub-grant signature	Sub-grant agreement signed; project formally initiated; initial work plan and administrative setup in place.
Interim payment	Up to 40% (covering M1–M4)	Month 5, after completion of M1–M4 activities	Successful completion and validation of intermediate deliverables and milestones defined for M1–M4, including the interim progress report.
Final payment	Remaining budget (M5–M8)	Within one month after project end	Final validation of all remaining deliverables, final report and evidence that objectives and KPIs have been achieved as per the approved proposal and sub-grant agreement.
*Exact dates are fixed in each sub-grant agreement based on the contractual project start date.			

For consortium projects, all three instalments are paid exclusively to the coordinator, who is responsible for internal distribution to partners according to the agreed budget split in the sub-grant and consortium agreements.

Although detailed financial cost reporting is not required under the lump-sum mechanism, beneficiaries must keep internal records and supporting documentation to justify the soundness of their budget estimation in case of audits or verifications by the European Commission or the CYberSynchrony consortium.

All reporting templates and mandatory deliverables are described in the Open Call Guidelines (Annex III - b).

9.3 Monitoring procedures and interaction with CYberSynchrony technical partners

Monitoring of the funded projects is carried out jointly by the Open Call Management Team (OCMT), with a focus on verifying progress against the agreed milestones, ensuring alignment with the project's cybersecurity objectives and supporting timely delivery of results.

Each funded project is assigned a primary technical contact from the OCMT. This contact organises a kick-off meeting at the end of M1, during which the work plan, deliverables, risks and integration expectations are reviewed and agreed. Thereafter, monthly remote progress meetings are held between the beneficiary and the assigned technical partner to review ongoing activities, discuss technical issues, and prepare for the interim and final reviews.

At the M4 interim checkpoint, each assigned technical partner from the OCMT validates the submitted deliverables and the interim report against the contractual work plan and the CYberSynchrony requirements. Any deviations, delays or risks are documented, and corrective actions are agreed together with the beneficiary before the interim payment is authorised. A similar joint review is carried out at the end of the project for the final deliverables and final report, providing the basis for the final payment decision.

From the beneficiary perspective, effective monitoring requires:

- timely participation in scheduled meetings;
- provision of concise progress updates and evidence for completed work;
- prompt responses to clarification or follow-up requests from the OCMT.

© CYberSynchorny, 2026

9.4 Management of deviations, underperformance and possible reduction/termination of support

Beneficiaries must inform the Coordinator without delay of any events or circumstances that may affect the implementation of their action, including delays, major technical problems, or changes in the work plan. Deviations identified through the progress meetings are first addressed through a corrective approach. The OCMT will request clarifications and, where appropriate, a short corrective plan with updated timing or technical adjustments, provided that the overall objectives and results of the sub-project remain achievable within the contractual duration. If the beneficiary delivers incomplete or inadequate outputs at M4 or at the final stage, the corresponding interim or final payment may be suspended or not released until the required deliverables are satisfactorily revised, in line with the conditions defined in the sub-grant agreement and the Digital Europe Programme rules.

In cases of serious or persistent breach of contractual obligations – such as non-implementation of essential tasks, refusal to provide information, or non-compliance with the sub-grant agreement – the Coordinator may apply the remedies foreseen in Article 4 ("Breach of contractual obligations"). These include formal notification of the breach, a 30-day period to remedy it where feasible, and, if the situation is not corrected, the possibility to terminate the agreement, reduce or cancel payments, and recover amounts already paid. The exact articles and legal effects are specified in the signed sub-grant agreement (ANNEX II - 6 and ANNEX II - 7).

9.5 Record-keeping, checks, audits and ex-post controls

Beneficiaries must keep adequate records and evidence to demonstrate that the sub-project has been properly implemented in line with the approved proposal and the sub-grant agreement. In particular, they must retain all documents necessary to show that the agreed activities, deliverables and milestones have been carried out (technical reports, deliverables, meeting minutes, test results, etc.) and that the eligibility conditions were respected for the entire duration of the action. These supporting records must be kept for up to five years after the final payment of the CYberSynchrony grant, in line with the underlying programme rules.

Article 11 ("Checks and reviews") of the sub-grant agreement clarifies that the European Commission, the European Court of Auditors, the European Anti-Fraud Office (OLAF) [4] and other authorised bodies may carry out checks, reviews, audits or investigations on the sub-grant and its implementation.

For the CYberSynchrony FSTP scheme, which uses a lump-sum model, these controls focus on verifying the technical implementation and the fulfilment of milestones and deliverables rather than auditing underlying cost items; beneficiaries have no obligation to document individual costs incurred for the sub-project.

Beneficiaries must therefore be prepared to provide, on request:

- The signed sub-grant agreement (and, where applicable, the consortium agreement and declarations of honour).
- All contractual deliverables and reports linked to the three lump-sum instalments.
- Internal evidence that the activities described in the proposal have been carried out (e.g. source code or technical documentation for tools, test reports, meeting records with the CYberSynchrony technical partners, training materials, etc.).
- Any other documentation explicitly requested in the sub-grant agreement or by the auditing body.
- During a check or review, beneficiaries are required to grant access to relevant documents and systems and to cooperate fully with the CYberSynchrony Coordinator and with the competent EU bodies. The results of checks, reviews or audits may lead to confirmation of the amounts, to

© CYberSynchorny, 2026

recommendations for future improvements, or, in serious cases of non-compliance, to a reduction or recovery of the contribution, in line with the procedures set out in the sub-grant agreement and the DEP legal framework.

9.6 Contact points and helpdesk

Throughout the FSTP lifecycle, beneficiaries and applicants have several formal contact channels with CYberSynchrony. The primary helpdesk for all questions related to the open calls, the submission platform and the financial support process is the Open Call Management Team (OCMT) coordinated by MAG. For any questions on procedures, documentation or issues encountered, beneficiaries can contact the OCMT via the official project email: ***info@cybersynchrony.eu***

This address is already used as the contact point in the D7.2 beneficiary feedback exercise and will also serve as the generic reference for FSTP-related queries. In addition, the CYberSynchrony website hosts two dedicated pages with up-to-date information and practical guidance:

The Open Calls page (https://cybersynchrony.eu/open-calls/), which provides the guidelines for applicants, the proposal template, the FAQ document, links to all legal and supporting documentation, and detailed instructions on accessing and using the submission platform.

The External Evaluators page (https://cybersynchrony.eu/external-evaluators-team/), which provides the timeline and specific information for external experts wishing to join the evaluator pool.

All proposals and evaluator applications are submitted exclusively through the CYberSynchrony online platform (https://cybersynchrony.grantplatform.com), which handles registration, uploads and server-time stamping of submissions.

© CYberSynchorny, 2026

10 Future actions for D7.3

D7.3 will be the second iteration of this deliverable once the open call sub-projects have been implemented. While D7.1 focuses on defining and documenting the information package, evaluation metrics and financial handbook in advance, D7.3 will complete the picture with evidence from actual implementation. In particular it will include:

1. The list of successful applicants for each of the three open calls, with basic descriptors such as beneficiary name, country, call and topic addressed, consortium composition (where applicable), total lump-sum awarded and of course the project title and acronym.

2. YouTube video links from each sub-project (minimum duration 8 minutes – maximum 12 minutes) as they are part of their mandatory deliverables. Each video will present each sub-project's objectives, highlight the main outcomes and results, and include a short demonstration of how the developed tool/module/algorithm/model/service/activities functions in practice.

3. The final results reports from all sub-projects: Each sub-project will have to produce a Final Results Report which will summarise the main achievements, technical outcomes, and impacts of the project. These reports are part of the mandatory deliverables of each sub-project and although it will be uploaded to a dedicated section of the CYberSynchrony website, it will also be part of D7.3 for sustainability purposes.

© CYberSynchorny, 2026

11 Conclusions

D7.1 consolidates the full framework needed to launch and operate the CYberSynchrony FSTP scheme complying with the Grant Agreement, transparent for applicants and manageable for the consortium. It brings together, the Beneficiary Information Package (guidelines, proposal template, FAQ), the complete set of legal instruments for both beneficiaries and external evaluators, the evaluation metrics and documentation, and the Beneficiary Financial Handbook covering the lump-sum model, payment schedule and monitoring arrangements.

© CYberSynchorny, 2026

12 References

[1] European Parliament and Council of the European Union, "Regulation (EU) 2021/694 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166," 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0694. [Accessed 13 2 2026].

[2] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. [Accessed 13 2 2026].

[3] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR), OJ L 119," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 13 2 2026].

[4] European Parliament and the Council of the European Union, "Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ L 248, 18.9.2013," 2013. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2013/883/oj. [Accessed 13 2 2026].

[5] European Commission, "Horizon Europe (HORIZON) Model Grant Agreement, Version 1.0," 2021. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/agr-contr/unit-mga_he_v1.0_en.pdf. [Accessed 13 2 2026].

[6] European Parliament and the Council of the European Union, "Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations," 2021. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2021/695/oj.

[7] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements," 2022. [Online]. Available: https://www.iso.org/standard/27001.html. [Accessed 13 2 2026].

© CYberSynchorny, 2026

Annex I – Legal documentation for external evaluators

Due to the large size of the documents, it is hard to include them in this deliverable.

All three annexes (Annex A – Contract for external evaluator (template), Annex B – Conflict of Interest, Annex C – Bank details) related to the legal documentation for the external evaluators can be downloaded from the CYberSynchrony website:

https://cybersynchrony.eu/wp-content/uploads/2025/12/External-Evaluators.zip

© CYberSynchorny, 2026

Annex II – Legal documentation for beneficiaries (FSTP)

Due to the large size of the documents, it is hard to include them in this deliverable.

All annexes (Annex 2a – Declaration of Honour (individual expert), Annex 2b – Declaration of Honour (universities, research organisations, or other public sector bodies), Annex 2c – Declaration of Honour SME (template), Annex 3 – SME Self-Declaration (template), Annex 4 – Bank account information (template), Annex 5 – Open Call Declaration of Honour - consortium agreement, Annex 6 – CYberSynchrony Sub-grant agreement for FSTP (for consortia), Annex 7 – CYberSynchrony Sub-grant agreement for FSTP (single entity)) related to the legal documentation for beneficiaries can be downloaded from the CYberSynchrony website:

https://cybersynchrony.eu/wp-content/uploads/2025/12/Legal-documentation-Open-call-applicants.zip

© CYberSynchorny, 2026

Annex III – Supporting documentation for Open Call beneficiaries and external evaluators

Due to the large size of the documents, it is hard to include them in this deliverable.

All annexes (Annex IIIa – Proposal technical template, Annex IIIb – Open Call guidelines for applicants, Annex IIIc – FAQ) related to the supporting documentation for beneficiaries and external evaluators can be downloaded from the CYberSynchrony website:

Proposal technical template: https://cybersynchrony.eu/wp-content/uploads/2025/12/Proposal-technical-template.docx

FAQ: https://cybersynchrony.eu/faqs-open-calls-fstp/

Open Call guidelines for applicants: https://cybersynchrony.eu/wp-content/uploads/2026/02/Open-Call-guidelines-for-applicants-v3.0.pdf

Although the "Open Call guidelines for applicants" document can be downloaded from the link provided above, it is provided here, since it contains critical information regarding the open calls and the external evaluators and describes in detail all necessary procedures, requirements and methodology that will be followed.

© CYberSynchorny, 2026

Open Call guidelines for applicants

Project: CYberSynchrony- Harmonising People, Processes & Technology for Robust Cybersecurity,
Grant Agreement Number: 101158555

https://cybersynchrony.eu/open-calls/

Funding Authority: European Union - Horizon Europe Framework Programme (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)

Call Identifier: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST

Date: 19-02-2026 – Version 6.0

Please carefully read this guide before submitting your application.

This document provides essential guidelines and detailed instructions for applicants interested in applying to the CYberSynchrony Open Calls for Financial Support to Third Parties (FSTP). It also contains valuable information related to the applicants who are interested in joining our external evaluators' team.

Funded by the European Union

CYberSynchrony project has received funding by the European Union's Digital Europe programme under Grant Agreement no. 101158555

Disclaimer

This document may contain material that is copyright of certain CYberSynchrony beneficiaries and may not be reproduced or copied without permission. All CYberSynchrony partners (*Table 1*) have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Table 1 CYberSynchrony Participants list

Number	Role	Short name	Legal name	Country
1	COO	MAG	MAGGIOLI SPA	IT
2	BEN	eBOS	EBOS TECHNOLOGIES LIMITED	CY
3	BEN	IANUS	IANUS TECHNOLOGIES LTD	CY
4	BEN	TRUST	TRUSTILIO BV	NL
5	BEN	UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER	GR
6	BEN	DSA	ARCHI PSIFIAKIS ASFALEIAS	CY
7	BEN	KETYAK	ETHNIKI YPIRESIA PLIROFORION	GR
8	BEN	FP	FOCAL POINT	BE
9	BEN	BYTE	BYTE COMPUTER ANONYMI VIOMICHANIKI EMPORIKI ETAIREIA	GR
10	BEN	EGL	DIMOS EGALEO	GR
11	BEN	MER	MERIDIAN SRL	IT
12	BEN	AMC	SAMOUTIS KAI SYNERGATES IEPE	CY

The information in this document is provided "as is" and no guarantee or warranty is given that fits for any particular purpose. The user thereof uses the information at its sole risk and liability. Moreover, it is clearly stated that the CYberSynchrony consortium reserves the right to update, amend or modify any part, section or detail of the document at any point in time without prior information. The CYberSynchrony project, funded from the European Union's DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST. Call foresees as an eligible activity the provision of financial support to third parties, as a mean to achieve its own objectives.

LEGAL NOTICE

The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Project number: 101158555
Project name: Harmonizing People, Processes, and Technology for Robust Cybersecurity
Project acronym: CYberSynchrony
Call: DIGITAL-ECCC-2023-DEPLOY-CYBER-04
Topic: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST
Type of action: DIGITAL-JU-GFS
Service: ECCC
Project starting date: fixed date: 1 June 2024
Project duration: 36 months

Contents

1. Overview 5
1.1. Submission Platform 5
1.1.1. For Open Call Applicants (proposal submission): 5
1.1.2. For External Evaluators (application to join the evaluator pool): 5
1.1.3. Further information 6
2. Brief description of the CYberSynchrony Open Calls 6
2.1. Open Call 1: Infrastructure Resilience & Operational Readiness 6
2.2. Open Call 2: Compliance, Innovation & Regulatory Advancement 7
2.3. Open Call 3: Mutual Assistance & Cyber Collaboration Among Member States 7
2.4. CYberSynchrony objectives 8
3. Funding details and Participation Rules 8
3.1. Reallocation of Remaining Funds and Reserve List 9
3.2. Eligible Cost Types (as part of Lump Sum) 10
3.3. Payment Modalities 10
3.3.1. Proposed Payment Structure 10
3.3.2. Coordination and Internal Fund Distribution 11
4. Duration and Possible Time Extensions 11
5. Eligible Applicants per Open Call 11
6. Proposal Evaluation Criteria 13
6.1. Scoring Scale and Threshold 13
6.2. Ranking and Tie-breaking Rules 14
6.3. Final Selection 14
6.4. Redress process 14
7. Proposal structure 15
8. Intellectual property rights (IPR) and results ownership 17
9. Conflict of Interest Rules 18
9.1. Open call applicants 18
9.2. External Evaluators 18
10. Sub-grant Agreement 18
10.1. Information on which documentation is mandatory to be submitted, and which should be taken into consideration 19
11. Core CYberSynchrony Modules 20
11.1. CYRESCUE – Resilience and Incident Response 20

11.2. CYBERRA – Threat Intelligence and Risk Analysis..... 21
11.3. CYBRITE – Continuous Monitoring and Early Threat Detection.....22
11.4. CROSS-CORE – Cross-Border Coordination and Secure Information Exchange 22
11.5. CYBERWISE – Cybersecurity Awareness and Behavioural Training.....23
11.6. CYBERGOPLUS – Governance, Standards, and Regulatory Compliance ... 24
12. Access to CYberSynchrony Public Deliverables 24

List of Changes

No of change	Section	Change	Implementation date
		VERSION 2.0	
1	V2.0: Section 11	Minor changes regarding the description of the CYberSynchrony modules	08-01-2026
		VERSION 3.0	
2	V3.0: Section 5	Private research institutes are added as eligible partners for OC1	09-02-2026
		VERSION 4.0	
3	V4.0: Section 5	Eligible countries list clarified – Since Objective 3 which is related to Cybersecurity calls excludes specific countries as defined in the DEP.	13-02-2026
		VERSION 5.0	
4	V5.0: Section 3	Section 3.2: The sentence: "Not provided by the CYberSynchrony consortium", was changed to "Expertise not provided by the consortium of the proposal" Section 3.2: The following sentence was also added: "Indirect costs 25% must also included – for more details check the proposal template"	17-02-2026
5	V5.0: Section 5	Table 5: During change no2, and for OC1, SMEs were accidentally deleted from private organisations: The revised and correct sentence is: "and private organisations [research, SMEs] operating within the NIS2 sectors"	
6	V5.0: Section 7	In Table 7 (Implementation plan section), and to be consistent with the mandatory deliverables given in the proposal template, it was added the "Detailed implementation/financial plan" (M1)	
7	V6.0: Section 5	Table 5: For OC1, and OC2, NGOs were also added as eligible partners. For OC3 – Mutual Assistance & Cyber Collaboration Among Member States, to assist the applicants, more clarifications were given regarding the entities' eligibility	19-02-2026

1. Overview

CYberSynchrony delivers an integrated, modular cybersecurity framework, combining advanced threat intelligence, automated response systems, and secure channels for cross-border collaboration:

a. Support rapid detection and mitigation of cyber incidents, continuous risk monitoring, and effective information sharing between Member States and key stakeholders.
b. Emphasise on fostering a cybersecurity-aware environment, offering targeted training, awareness campaigns, and practical tools that support organisations in aligning with evolving regulatory requirements (i.e. NIS2 Directive).

Through its 3.55m € Open Call (which will comprise 3 different open calls), CYberSynchrony invites SMEs, innovators, and specialised teams to contribute tools, services, and practices that can enhance the project's platform and expand its applicability across different sectors. This financial support mechanism offers the opportunity to integrate new capabilities into real-world pilots, ensuring the solutions developed are practical, scalable, and relevant to the security needs of Europe's digital infrastructure.

For more information regarding the CYberSynchrony's modules and architecture, please refer to section 12.

Open Call submissions – Timeline

CYberSynchrony will launch the calls together with all necessary documentation (templates, guidelines, submission platform, etc), on the **1st of January 2026**. All three Open calls will run simultaneously, whilst they will remain for proposal submissions for a period of two months. Therefore, all interested applicants must submit their completed applications no later than the **1st of March 2026, 17:00 CET**.

The rest of the dates regarding periods related to proposal evaluation, contract signing, and Open call projects starting dates, are given on the CYberSynchrony's website:

https://cybersynchrony.eu/open-calls/

External evaluators applications – Timeline

The CYberSynchrony project is looking to form a team of external evaluators to review the submitted Open Call proposals. The call for external evaluators will have a starting date which will be the **1st of January 2026** and the interested applicants must submit their completed applications no later than the **15th of February 2026, 17:00 CET.**

The rest of the dates regarding periods related to selection of the right candidates, contract signing period, and evaluation start/end dates, are given on the CYberSynchrony's website:

https://cybersynchrony.eu/external-evaluators-team/

1.1. Submission Platform

All Open Call Applicants (FSTP) and External Evaluators must use the CYberSynchrony dedicated online platform for their respective submissions/applications.

Platform link: https://cybersynchrony.grantplatform.com , ***Registration required***

1.1.1. For Open Call Applicants (proposal submission):

Proposals must be submitted exclusively through the platform. Applicants may edit their proposal after initial submission; however, no further changes will be possible after the submission deadline. Submissions sent by any other means (e.g., email) will not be accepted for evaluation.

1.1.2. For External Evaluators (application to join the evaluator pool):

Applications must be submitted exclusively through the platform. Evaluators may edit their application after initial submission; however, no further changes will be possible after the application deadline and the submission process will be locked.

1.1.3. Further information

All call-related documentation and supporting material, including detailed guidance on platform access, account creation, and step-by-step instructions for both Open Call Applicants and External Evaluators, is available at the dedicated CYberSynchrony Open Calls webpage: https://cybersynchrony.eu/open-calls/

This webpage also includes a YouTube tutorial demonstrating how to use the platform to (i) submit an Open Call (FSTP) application and (ii) apply as an external evaluator. Users are encouraged to review the available material and register on the platform early, well in advance of the applicable deadlines.

All deadlines are based on the **official platform server time (CET)**. Submissions/applications are deemed received only when successfully submitted and **time-stamped by the server**. The user's local device time, time zone settings, or location will not be taken into account.

It is strongly recommended not to wait until the last minute to submit the proposal. Failure of the proposal to arrive in time for any reason, including network communications delays or working from multiple browsers or multiple browser windows, is not acceptable as an extenuating circumstance. The time of receipt of the application as recorded by the submission system will be definitive.

2. Brief description of the CYberSynchrony Open Calls

The CYberSynchrony project will launch **three open calls** under its Financial Support to Third Parties (FSTP) scheme. These calls are designed to bring in external expertise, services, and tools to reinforce key aspects of the project platform and to support cybersecurity deployment across NIS2 sectors. The total available budget for FSTP is **€3,550,000**, and no third party may receive more than **€200,000 in total**, even if selected under multiple calls. Each third party can participate in only one proposal per call.

Each call supports a defined set of **specific topics**; their brief description is given below. In case of tools/solutions/models developed throughout the duration of the FSTP projects, these are expected to reach TRL 7.

2.1. Open Call 1: Infrastructure Resilience & Operational Readiness

Scope

This call targets the enhancement of cybersecurity infrastructure and operational readiness specifically within sectors governed by the NIS2 Directive—energy, transport, drinking water supply and distribution, and manufacturing. It supports solutions aimed at improving sector-specific resilience against cyber threats and enabling rapid, coordinated responses.

Priority Areas (all priority areas must be met)

1. **Strengthening Sector-specific Cybersecurity Operations:** Support initiatives that establish or amplify operational cybersecurity hubs tailored to the unique needs of energy, transport, water supply, and manufacturing sectors, ensuring sector-specific threat intelligence gathering, rapid incident response, and best practice sharing.
2. **Enhanced Threat Intelligence and Risk Assessment for NIS2 Domains:** Channel funds towards projects that aim to develop or adapt advanced threat intelligence platforms specific to the challenges of energy, transport, drinking water, and manufacturing sectors. Focus on real-time monitoring, predictive analytics, and proactive threat hunting tailored to the infrastructures of these domains.
3. **Promotion of Cybersecurity Awareness in NIS2 Sectors:** Fund campaigns and training programs tailored to professionals and stakeholders in the energy, transport, water, and manufacturing sectors. Promote best practices, risk mitigation, and cybersecurity hygiene specific to each sector's challenges and requirements.
4. **Supporting Cross-sector Collaborations:** Encourage projects that foster inter-sector collaboration, ensuring best practices in one domain (e.g., energy) can be shared and adapted for others (e.g., transport or water supply).

Linked CYberSynchrony Objectives (see section 2.4): #1, #3, #6, #7, #8
Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of essential entities supported
- Number of threat assessments/risk scenario analyses carried out
- Number of risk monitoring services provided

2.2. Open Call 2: Compliance, Innovation & Regulatory Advancement

Scope

This call addresses the regulatory landscape and supports innovative cybersecurity solutions specifically tailored for sectors covered by the NIS2 Directive—energy, transport, drinking water supply and distribution, and manufacturing.

Priority Areas (all priority areas should be met)

1. **Encouraging Regulatory Compliance in NIS2 Sectors:** Dedicate funding to support initiatives focusing on achieving and maintaining compliance with cybersecurity regulations specific to energy, transport, water supply, and manufacturing sectors within the EU.
2. **Boosting Innovations Tailored to NIS2 Domains:** Support research and development projects addressing the unique cybersecurity challenges and needs of the specified sectors. This includes creating sector-specific tools, technologies, and strategies ensuring a secure operational environment.
3. **Promotion of Cybersecurity Awareness in NIS2 Sectors:** Fund campaigns and training programs tailored to professionals and stakeholders in the energy, transport, water, and manufacturing sectors. Promote best practices, risk mitigation, and cybersecurity hygiene specific to each sector's challenges and requirements.
4. **Supporting Cross-sector Collaborations:** Encourage projects that foster inter-sector collaboration, ensuring best practices in one domain (e.g., energy) can be shared and adapted for others (e.g., transport or water supply).

Linked CYberSynchrony Objectives (see section 2.4): #6, #8, #9
Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of penetration tests provided
- Number of essential entities supported
- Number and nature of vulnerabilities discovered

2.3. Open Call 3: Mutual Assistance & Cyber Collaboration Among Member States

Scope

In an era where cybersecurity threats transcend borders, the collaboration between Member States (MS) is pivotal. This Open Call seeks to foster a more integrated and united approach to cybersecurity, emphasizing mutual assistance, best practice sharing, and coordinated response mechanisms among MS.

Priority Areas (Proposals must clearly address at least one of the listed priority areas and detail how the initiative will enhance mutual assistance among Member States)

1. **Establishing Unified Threat Intelligence Platforms:** Develop or enhance platforms that facilitate real-time sharing of threat intelligence between MS, ensuring a collective response to emerging cyber threats.
2. **Joint Cybersecurity Exercises & Training:** Organize joint cybersecurity exercises simulating cross-border incidents, aiming to test and improve the collective response capabilities of MS. Promote training sessions where MS can share their unique experiences, tools, and best practices, ensuring that all states benefit from individual advancements.
3. **Incident Response Coordination:** Create or amplify mechanisms that enable rapid coordination between MS when a cybersecurity incident impacts multiple countries. Develop shared playbooks

and protocols to guide coordinated responses, ensuring faster containment and mitigation of threats.

Linked CYberSynchrony Objectives (see section 2.4): #2, #4, #5

Mandatory KPIs to be defined by the applicants (additional KPIs may be defined):

- Number of potential number of users covered per test/ exercise
- Number of cross-border actions/exercises

2.4. CYberSynchrony objectives

Each FSTP application is mandatory to be aligned with some of the project's objectives, according to which open call the applicant wishes to submit to (1, 2 or 3). The objectives that the FSTP projects should be aligned with, are mentioned in Sections 2.1 (Open call 1), 2.2 (Open call 2) and 2.3 (Open call 3).

OBJ1: Improve threat and risk assessment through the use of advanced threat intelligence platforms, analytics tools, and risk assessment methods. The objective is to enable more accurate detection and proactive mitigation of cyber threats targeting essential services and digital infrastructure

OBJ2: Minimize the duration and impact of cyber incidents by integrating orchestration and automation into incident response coordination. This includes automating repetitive tasks and streamlining workflows to improve containment speed and efficiency

OBJ3: Strengthen risk monitoring and early incident detection using advanced cybersecurity analytics. This includes analysing network activity, software integrity, user behaviour, and system performance to identify anomalies and potential threats

OBJ4: Enhance mutual assistance among Member States and enable more realistic and frequent cross-border cyber exercises through the deployment of virtual cyber range platforms that simulate complex cyberattack scenarios and behavioural challenges

OBJ5: Ensure data privacy and secure communication during information sharing between Member States by establishing an encrypted and standardised communication infrastructure for threat intelligence, incident data, and best practices

OBJ6: Foster collaboration and knowledge sharing among stakeholders in the cybersecurity ecosystem by enabling real-time exchange of information and experiences to collectively strengthen cyber capabilities across the EU

OBJ7: Enhance early detection and response to cyber incidents by leveraging advanced threat intelligence and analytics while reducing the impact of potential cyber threats on critical infrastructure and essential entities

OBJ8: Promote cybersecurity awareness and behavioural change by implementing educational programs, training activities, and awareness campaigns targeting citizens, organisations, and businesses to cultivate a security-conscious society

OBJ9: Ensure high and consistent levels of cybersecurity across the EU by promoting comprehensive policies, supporting regulatory alignment, encouraging standardisation and certification, and facilitating dissemination and training across sectors

3. Funding details and Participation Rules

All financial support will be provided in the form of **lump sum grants**, in accordance with Article 6 of the Horizon Europe Model Grant Agreement. Funding is not based on reimbursement of actual costs but on the successful completion of predefined technical milestones and deliverables.

As no differentiation is made by entity type in the Grant Agreement, the funding scheme applies **equally to all beneficiaries**, regardless of their legal status (e.g., SMEs, research centres, higher education institutions, non-profit organisations, public entities, individuals). Applicants are required to define a realistic work plan and budget in line with the applicable funding caps described in Tables 1, 2, and 3.

The CYberSynchrony project allocates **€3,550,000** under the Financial Support to Third Parties (FSTP) mechanism, divided across three open calls. Financial support is granted in the form of **lump sum payments**, disbursed upon successful delivery of predefined outputs (deliverables), rather than based on actual incurred costs. Applicants must comply with the funding conditions defined in **Table 2, Table 3, and Table 4**.

Table 2 Main funding rules

Rule	Provision
Maximum funding per third party	€200,000 (across all open calls combined)
Proposal limit per each call	One proposal per third party
Multiple participations in the same Open Call	Disqualifies all such proposals
Funding scheme	Lump sum, tied to output verification

Table 3 Funding Range by Open Call according to consortium size, total budget allocation and estimated no. of proposals

Open Call	Consortium size	Min–Max funding	Total Budget Allocation	Estimated Number of Funded Proposals
Call 1 – Infrastructure & Operations	Single Entity Consortium (2 or 3)	€65,000 – €200,000 €100,000 – €200,000	€1,200,000	6–9 proposals
Call 2 – Compliance & Innovation	Single Entity Consortium (2 or 3)	€70,000 – €200,000 €120,000 – €200,000	€1,200,000	6–9 proposals
Call 3 – Cross-border Coordination	No single entity is allowed Consortium (2 or 3)	€100,000 – €200,000	€1,150,000	6–9 proposals

Table 4 shows the caps on specific expense categories. Participants should pay attention to these limits so that none is exceeded. For each call, the consortium should justify expenses in all 3 categories, but keeping in mind the budget limits showed in Table 2 and Table 3.

Table 4 Thematic Sub-caps per Open Call

Call	Activity Type	Maximum Allowed
Call 1	Infrastructure & Operational Set-up	€ 120,000
	Threat Intelligence Platform Development/adaptation	€ 65,000
	Incident Response Mechanisms	€ 55,000
Call 2	Regulatory Compliance Initiatives	€ 90,000
	R&D for Cybersecurity Challenges	€ 80,000
	Development of Sector-specific Tools & Strategies	€ 70,000
Call 3	Threat Intelligence Platforms (Cross-border)	€ 100,000
	Joint Exercises and training	€ 80,000
	Incident Response Coordination	€ 70,000

3.1. Reallocation of Remaining Funds and Reserve List

In cases where an open call concludes with unallocated funds—either due to undersized budgets of selected proposals or an insufficient number of qualifying applications—the remaining budget will not be discarded. Instead, residual funds from all open calls will be consolidated into a common reserve pool.

A fixed reserve list of three proposals per open call will be maintained. These will be the next highest-ranked proposals that have met all eligibility and evaluation thresholds but were not initially selected for funding.

Should budget become available—either from within a specific call or the combined reserve pool—the consortium may fund one or more reserve list proposals in strict ranking order, provided that:

- The proposal meets all eligibility and threshold requirements.
- Its funding request does not exceed the available remaining budget (no partial grants will be awarded).

3.2. Eligible Cost Types (as part of Lump Sum)

The following categories of activities are explicitly eligible for financial support (Indirect costs 25% must also included – for more details check the proposal template):

- **Personnel:** Costs related to participation in CYberSynchrony activities, project work, training, and collaboration.
- **Travel:** Expenses for attending meetings, events, or conferences related to the project.
- **Technical Resources:** Acquisition or use of necessary hardware, software, and datasets.
- **Infrastructure:** Access fees or usage costs essential to project implementation.
- **Subcontracting:** Permitted only if:
  - Defined clearly in the proposal,
  - Expertise not provided by the consortium of the proposal,
  - Directly related to the project objectives.
- **Communication:** Audio/visual materials and outreach tools.
- **Promotion:** Efforts to disseminate and promote the supported services and CYberSynchrony outcomes

3.3. Payment Modalities

Financial support to third parties under the CYberSynchrony open calls will be provided in the form of **lump sum grants**. The awarded amount will not be reimbursed based on actual incurred costs, but rather disbursed upon verification that specific deliverables — as defined in the funded proposal — have been completed.

This lump sum model applies to all types of activities supported under the open calls, including those carried out by individual applicants or by consortia. The exact amount of the grant and the conditions for payment will be specified in the sub-grant agreement signed between the third party and the CYberSynchrony consortium.

While CYberSynchrony provides funding under the lump sum model for selected third parties, applicants should be aware of the standard principles applied when estimating their project budget. Even though **actual costs will not be reimbursed**, and no detailed financial reporting is required during project execution, beneficiaries must be prepared to justify their cost calculations in the event of a verification or audit by the European Commission. For this reason, it is recommended that all applicants retain supporting financial documentation for their internal records.

3.3.1. Proposed Payment Structure

Payments will be made in lump sums, strictly tied to the achievement and validation of predefined deliverables and milestones, as described in the Sub-grant Agreement. To maintain effective project implementation and cash flow management, the lump sum awarded will typically be split into three instalments:

1. Prefinancing (30% of the total budget) – Month 1 (Total duration of the project will be 8 months)

- Paid within one month after signing the Sub-grant Agreement and project initiation.

2. Interim Payment (up to 40% of the total budget for Months M1-M4) (Payment will take place in M5 after checking that all deliverables have been structured according to the plan - Total duration of the project will be 8 months)

- Paid upon successful completion and validation of intermediate project milestones and deliverables, clearly defined at the beginning of the project (e.g., mid-term reports, intermediate technical or implementation deliverables).

3. Final Payment (remaining budget for months M5-M8) – paid within 1 month after the end of the open call project

- Released upon the final validation of all remaining deliverables and the final report, demonstrating complete implementation and achievement of the project objectives.

3.3.2. Coordination and Internal Fund Distribution

In consortium-led proposals (i.e. involving more than one beneficiary), financial disbursements follow a **centralised distribution model**:

All instalments of the lump sum—prefinancing, interim, and final—are paid **exclusively to the lead partner (coordinator)**. This aligns with standard FSTP practice, where acknowledging one primary legal and financial point of contact simplifies administration and accountability.

The coordinator assumes full responsibility for allocating the funds internally to the consortium members. This distribution should adhere to the **pre-planned budget breakdown** agreed upon during proposal development and reflected in the Sub-grant Agreement. The **consortium agreement** must specify the percentages or amounts allocated to each partner.

4. Duration and Possible Time Extensions

The duration of the FSTP projects funded under the CYberSynchrony open calls is fixed to 8 months and the starting date will be clearly defined at the moment of the sub-grant agreement signature. However, in exceptional and duly justified cases (e.g., unforeseen technical delays, significant external factors beyond the beneficiary's control), the Open Call Management Team (OCMT)[1] may approve a one-time extension of the project duration by up to one month – (this will also depend to other unforeseen delays that may happen before the initiation of the FSTP projects, for example: delays in the evaluation, contract signing, etc.).

Beneficiaries seeking such an extension must submit a written request at least one month before the original end date, providing detailed justification and demonstrating that the extension will ensure successful completion of all remaining deliverables. The OCMT will evaluate each request individually and reserves the right to approve or reject extension requests based on their assessment of the circumstances and justification provided. No additional funding will be provided for extended periods, and extensions must not exceed a total duration increase of one month. In the case of an extension, the final payment will be made one month after the end of the new extended ending period, and only if all deliverables have been submitted and their content aligns with what has been described in the proposal.

5. Eligible Applicants per Open Call

General Eligibility Conditions (Applies to all three Open Calls): Eligible applicants are entities established in countries as defined in the Digital Europe Programme (DEP) which include:

[1] OCMT (Open Call Management Team) is responsible for the design and specifications of the Open Calls, and supervising the implementation of the methodology phases as detailed in the grant agreement. This team is coordinated by MAG (MAGGIOLI SPA) and will include technical representatives from the CYberSynchrony consortium. OCMT will be responsible for the recruitment of the external evaluation experts to be involved in the evaluation process and the provision of content for the promotion of the Open Calls implementation.

a. the 27 EU Member States,
b. the European Economic Area (EEA) countries (Iceland, Liechtenstein, Norway)

Each third party may submit only one proposal per call. A third party may receive a maximum of €200,000 total across all open calls.

Large companies are excluded from these open calls.

In case of monobeneficiary (single entity) projects, the applicant must be an SME.

In case of consortia of 2 or 3 entities, the coordinator must be an SME and will be responsible for the payments of the other partners of the consortium. The consortium may have additional SMEs (excluding the SME acting as the coordinator), if necessary, for the scope of the FSTP project. In this case, the legal documentation related to the SMEs must be filled in by all SMEs.

The consortium agreement will be legally bound by signing the Annex 5 - Open Call Declaration of Honour - consortium agreement (HERE).

Error! Not a valid bookmark self-reference. shows the types of the applicants that can participate depending on the open call.

Table 5 Applicant eligibility based on the open call

Open Call	Eligible Participants
Call 1 – Infrastructure Resilience & Operational Readiness	• Cybersecurity firms (SMEs only – can be more than one, but one of these SMEs must act as the coordinator) specialising in infrastructure resilience • Public & competent authorities [ministries and government departments; regional and municipal authorities and their agencies; regulators and national CERT/SOCs; public hospitals; public universities and research institutes], NGOs, and private organisations [research, SMEs] operating within the NIS2 sectors • Independent cybersecurity professionals [Individuals] with experience in sector-specific operations and infrastructure
Call 2 – Compliance, Innovation & Regulatory Advancement	• Organisations [SMEs, Public entities, NGOs] involved in regulatory compliance, and/or • Research institutions, or tech startups focused on cybersecurity innovation in NIS2 sectors, and/or • Regulatory experts [SMEs, Public entities, Individuals] and cybersecurity innovators [SMEs, Public entities, Individuals] specialised in the relevant domain
Call 3 – Mutual Assistance & Cyber Collaboration Among Member States	• The coordinating participant must be an SME and must represent or be affiliated with a Member State's government, relevant cybersecurity agency, or a recognized research institution. • To demonstrate the cross-collaboration requirement for this call, the involvement of at least one additional partner from a different MS than the coordinating participant (any type of entities as stated in OC1 and OC2, excluding individuals) is mandatory. • Demonstrated experience in international cyber collaboration or mutual assistance initiatives is an advantage. • Proposals must clearly address at least one of the listed priority areas (see section 2.3) and detail how the initiative will enhance mutual assistance among Member States.

All participants should have a valid VAT and PIC number (including the individuals who are eligible to participate in Open Call 1 and Open Call 2).

6. Proposal Evaluation Criteria

All proposals submitted under the CYberSynchrony open calls will be evaluated by two independent external experts. Evaluations will be based on four criteria, each scored from **0 to 5**, with a minimum threshold of **3 out of 5 per criterion** required for eligibility (Table 6).

Table 6 Evaluation Criteria

Criterion	Description
1. Relevance and Excellence	The proposal must clearly define the project objectives and demonstrate their relevance to CYberSynchrony. It should address specific cybersecurity vulnerabilities, describe the main goals, and show alignment with the open call objectives and KPIs.
2. Methodological Soundness	The proposal must provide a clear and logically structured methodology explaining how the proposed objectives will be achieved. This includes a breakdown of the technical and operational approach, explanation of tools and frameworks to be used, sequencing of activities, interdependencies, and validation steps. The methodology should demonstrate that the applicant has a concrete, realistic, and technically credible plan for executing the work. Alignment with the CYberSynchrony architecture and integration of relevant modules should be made explicit where applicable. Evaluators must be able to understand not just what the applicant aims to do, but exactly how they will carry it out in practice.
3. Ambition and Impact	The proposal should show a clear ambition and expected outcomes, demonstrating the technical, operational, and market-level impact. Results must contribute to the goals and KPIs defined in each CYberSynchrony open call (there are separate sections for each call (Open Call 1: Section 2.1, Open Call 2: Section 2.2, Open Call 3: Section 2.3).
4. Implementation/ Team Skills and Expertise	A credible and structured implementation plan must be presented, including a realistic timeline (describe WP and tasks, always having in mind the "lump sum" approach), defined milestones and deliverables, and effective risk mitigation measures. Inadequate justification of costs and resources will result in a below-threshold score. Applicants must demonstrate that their team possesses the required knowledge and experience, including technical and regulatory expertise relevant to the targeted NIS2 sectors. Prior experience in cybersecurity innovation or deployment should be clearly described as well as their role in the project.

6.1. Scoring Scale and Threshold

For each criterion, a maximum of **5 points** will be granted, on a scale from 0 to 5 and with increments of 0.5. The **overall maximum score** is 20 points.
The individual scores are interpreted as follows:

- **0 – Fail**: The proposal fails to address the criterion or cannot be judged due to missing/incomplete information.
- **1 – Poor**: The criterion is inadequately addressed, with serious inherent weaknesses.
- **2 – Fair**: The proposal broadly addresses the criterion, but significant weaknesses remain.
- **3 – Good**: The criterion is well addressed, although improvements are necessary.
- **4 – Very Good**: The proposal addresses the criterion very well, with only minor improvements needed.
- **5 – Excellent**: All relevant aspects of the criterion are successfully addressed; shortcomings are negligible.

A **threshold of 3 out of 5 per criterion** is required for a proposal to qualify for selection. It is noted that **inadequateness of the justification on costs and resources**, as judged by expert evaluators, will result in a **below-threshold score in the Implementation category**.

6.2. Ranking and Tie-breaking Rules

Proposals will be ranked by their total score. In case of ties, evaluators will apply the following sequence of prioritisation criteria:

- **Rule 1:** Priority will be given to innovation of the concept (Criterion 1 – see Table 6).
- **Rule 2:** In case following Rule 1 there are proposals in the same position, priority will be given to proposals that their technology better fit to CYberSynchrony scope (Criterion 2 – see Table 6).
- **Rule 3:** In case following Rule 2 there are proposals in the same position, priority will be given to proposals that have higher impact and market potential (Criterion 3 – see Table 6).
- **Rule 4:** In case following Rule 3 there are proposals in the same position, priority will be given to the application that has lower funding request.
- **Rule 5:** In case following Rule 4 there are proposals in the same position, priority will be given to the number of female researchers participating in the team.
- **Rule 6:** In case following Rule 5 there are proposals in the same position, priority will be given to the application that increases CYberSynchrony project footprint in Europe.

If proposals are still ranked identically after applying these factors, an additional evaluator from the external evaluators' pool, will be appointed to re-evaluate the tied submissions and break the tie. A reserve list of the highest ranked proposals (after the funded ones) will be maintained, in case that any of the applicants of the successful proposals withdraw or fail to fulfil contractual obligations.

6.3. Final Selection

The CYberSynchrony Open Call Management Team (OCMT) will gather the reviews from the external evaluators. All reviews will be checked for accuracy (or errors) and consensus meetings will be held with the external evaluators if any inconsistencies are identified in order to eliminate inconsistencies and maximise clarity. After this, the provisional successful list of the awarded proposals will be documented, and all applicants will receive notification of the results accompanied with an Evaluation Summary Report (ESR). If the number or quality of eligible proposals is insufficient, the CYberSynchrony consortium has the right to re-open the call at a later date.

6.4. Redress process

The applicants who will receive a rejection letter, will have 3 working days to submit a request for redress, limited to eligibility errors or procedural issues affecting the evaluation. In that case, an internal review committee of the OCMT will examine the request for redress. The OCMT's role is to ensure a coherent interpretation of such requests, and equal treatment of applicants.
Requests must be:

- Related to the evaluation process or eligibility checks.
- Clearly describe the complaint.
- Received within the time limit (3 working days) from the reception of a rejection letter considering the proposal as non-eligible or the ESR information letter delivered.
- Sent by the applicant legal representative that has also submitted the proposal.

The committee will review the complaint and will recommend an appropriate course of action. If there is clear evidence of a shortcoming that could affect the eventual funding decision, it is possible that all or part of the proposal will be re-evaluated.
Please note:

- This procedure is concerned only with the evaluation and/or eligibility checking process. The committee will not call into question the scientific, technical or impact judgement of appropriately qualified experts.

- A re-evaluation will only be carried out if there is evidence of a shortcoming that affects the final decision on whether to include the partner in CYberSynchrony consortium or not. This means, for example, that a problem relating to one evaluation criterion will not lead to a re-evaluation if a proposal has failed anyway on other criteria.
- The evaluation score following any re-evaluation will be regarded as definitive. It may be lower than the original score.
- Only one request for redress per proposal will be considered by the committee. All requests for redress will be treated in confidence and must be sent to the OCMT at info@cybersynchrony.eu.

7. Proposal structure

Applicants must submit a concise proposal document that clearly presents the objectives, methodology, relevance, and expected impact of the proposed work. The proposal must be written in **English** and submitted in **PDF format** through the official CYberSynchrony submission platform (see section 1.1).

The maximum length of the proposal is **10 pages** (excluding any required annexes). Proposals exceeding this limit **will be considered ineligible and will be not evaluated.**

To facilitate fair and consistent evaluation, applicants are strongly encouraged to structure their proposal using the following format. Please keep the following information as a guideline on what information you should provide in order your proposal to be competitive (The template for your proposal can be downloaded from HERE). Each section is aligned with the evaluation criteria used by the reviewers (Table 7):

Table 7 Content description of each proposal section and corresponding linked criteria (see ***Table 6***)

Section	Content Description	Linked Evaluation Criterion
1. Executive Summary	Provide a high-level summary of the proposal, including the selected open call, the main cybersecurity challenge being addressed, the proposed solution, key activities, expected outcomes, and total requested funding. This section should give evaluators a complete snapshot of what the project is about and its strategic relevance.	***(All criteria – contextual overview)***
2. Project Objectives and Alignment	Clearly state the specific objectives of the proposal and explain how they respond to the priorities and scope of the selected open call. Indicate which CYberSynchrony project objectives (OBJ1–OBJ9, see 2.4) and KPIs the proposal contributes to. Make the connection between the sectoral challenge and the proposed approach explicit.	**Relevance and Excellence**
3. Technical and Methodological Approach	Describe in detail *how* the proposed objectives will be achieved. Include your methodological framework, selected tools or technologies, implementation logic, and key phases or work packages. Explain how CYberSynchrony modules (e.g. CYRESCUE, CYBERRA, etc) will be used, extended, or integrated. This section should show technical depth and internal coherence.	**Methodological Soundness**
4. Implementation Plan	Outline the structure and flow of work across the project duration. Include a realistic timeline, key tasks, list of milestones and deliverables, resource allocation, and risk mitigation strategies. If a consortium is proposed, specify the roles and responsibilities of each partner and their coordination plan. As part of our dissemination strategy, each FSTP project must include in its deliverables list (expected to be submitted at the end	**Implementation**

of the FSTP project (M8)) a demo video of their solution, a "final results" report and a "Detailed implementation/financial plan":

1. Demo video: Each funded project must prepare a presentation video (minimum duration 8 minutes – maximum 12 minutes) as part of its final reporting. The video should clearly explain the project's objectives, highlight the **main outcomes and results**, and include a **short demonstration** of how the developed tool/module/algorithm/model/service/activities functions in practice. The presentation should be structured for both technical and non-technical audiences, using clear visuals and narration. The final video must be submitted in **MP4 format (Resolution: 1920 × 1080 (Full HD, 16:9), Frame rate**: 25), and will be published on the CYberSynchrony website/social media for dissemination purposes.

2. Final Results Report (PDF/DOCX): Each funded project must prepare a **Final Results Report** in PDF and DOCX format, which will summarise the main achievements, technical outcomes, and impacts of the project. The report will be uploaded to CyberSynchrony's website, and will be publicly accessible. Hence, please ensure that not confidential information is included in it. The report should be around **2,000 words** in length and must include a **2000-character summary (including spaces)** that will be used for dissemination purposes. The report should also include **figures, diagrams, screenshots, or other visual elements** to make the results more accessible and engaging. Font size and type, margins and other layout rules, are the same as used in the proposal template.

To ensure uniformity, the report should follow the structure below:

1. **Cover Page**
   - Project title, acronym, beneficiaries, contact person.
2. **Executive Summary (2000 characters including spaces)**
   - Concise overview of objectives, results, and significance.
3. **Introduction and Objectives**
   - Brief context, problem addressed, project goals.
4. **Methodology and Technical Approach**
   - How the work was carried out (methods, tools, integration with CYberSynchrony modules).
5. **Main Results and Achievements**
   - Description of the key results, innovations, or demonstrators.
   - Include figures, screenshots, and technical evidence.
6. **Impact and Relevance**
   - Expected or achieved impact (technical, regulatory, sectoral, or market).
   - Contribution to CYberSynchrony objectives and KPIs.
7. **Conclusions and Next Steps**
   - Lessons learned, sustainability, and future exploitation potential.

3. Detailed implementation/financial plan: Apart from your technical deliverables that should be stated in your Work Packages,

	you have to include a deliverable entitled: "Detailed implementation/financial plan" (Delivery month: M1). In this deliverable you will have to provide a more detailed implementation/financial plan than what you will provide in your proposal, split per partner (all cost categories, Person Months, etc) and per payment period. More instructions and a template for this will be provided before the initiation of the projects.	
5. Expected Impact	Present the technical, operational, regulatory, or market impact of your proposed work. Clarify how the results will improve cybersecurity resilience, readiness, or compliance in the selected NIS2 sector(s). Reference the call-specific KPIs and describe any expected benefits across borders or sectors.	**Ambition and Impact**
6. Team and Organisational Capacity	Provide short profiles of the applicant(s) as entities (not description of CVs of the team), highlighting relevant experience, technical expertise, and sectoral knowledge. Emphasise any previous participation in cybersecurity projects or regulatory initiatives. For collaborative proposals, explain how the team composition enhances the proposal's strength.	**Team Skills and Expertise**
7. Budget Overview	Specify the total lump sum requested and provide a high-level distribution across main activities (e.g. personnel, software, training). Justify how the requested amount relates to the scope and effort involved. Respect the funding limits and sub-caps described in Tables 1, 2, and 3. No detailed cost breakdown is needed, but the budget must appear proportionate and credible.	**Implementation**

8. Intellectual property rights (IPR) and results ownership

Third-party beneficiaries funded under the CYberSynchrony Financial Support to Third Parties (FSTP) mechanism will retain ownership of all results they generate during the implementation of their funded projects. This includes, but is not limited to, software, data, algorithms, designs, prototypes, training materials, and documented methodologies developed with FSTP support.
However, in line with Horizon Europe obligations and the principles of open innovation and public value, the following conditions will apply:

1. Ownership and Responsibility

- All results produced by a single beneficiary belong solely to that beneficiary.
- In collaborative projects, ownership arrangements must be clearly agreed upon and described in a consortium agreement or internal partnership declaration.
- The above does not exclude the possibility for specific agreements to be made between the Beneficiary and one or more of the partners of CYberSynchrony.
- Beneficiaries are solely responsible for ensuring the protection of their results where appropriate (e.g., through patents, copyright, or trade secrets) and for managing any potential conflicts or shared ownership issues.

2. Access Rights for CYberSynchrony and the European Commission

- The CYberSynchrony consortium and the European Commission will be granted non-exclusive, royalty-free rights to access the results for purposes of:
  - Monitoring and verifying project implementation,
  - Dissemination of non-confidential information and success stories,
  - Ensuring policy alignment and program evaluation.
- This access is strictly for non-commercial and public-interest use and does not affect the beneficiary's commercial exploitation rights.

3. Exploitation and Use of Results

- Beneficiaries are encouraged to actively exploit their results beyond the funding period. This may include commercial use, standardisation activities, integration into existing product portfolios, licensing to third parties, or contributing to open-source ecosystems where relevant.
- The exploitation route should be compatible with the objectives of the CYberSynchrony project and the NIS2 Directive sectors targeted in the open calls.

4. Licensing and Third-Party Use

- Any licenses granted by beneficiaries to third parties must not restrict the access rights of the CYberSynchrony consortium or the European Commission as described above.
- Licenses must respect applicable intellectual property laws and must not compromise security-sensitive components, if such restrictions apply.

5. Confidentiality and Dissemination

- While results may be used for dissemination and public communication, confidential or security-sensitive information will not be shared without explicit consent from the beneficiary.
- The CYberSynchrony consortium may request non-confidential summaries of the results for use in project-level reporting and communication.

9. Conflict of Interest Rules

9.1. Open call applicants

The applicant must take all measures to prevent any situation where the impartial and objective implementation of the proposed tasks are compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest ('conflict of interests').

They must formally notify to the CYberSynchrony coordinator without delay any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation. The CYberSynchrony coordinator may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

9.2. External Evaluators

All evaluations of proposals submitted to the CYberSynchrony Open Calls will be carried out under strict conflict of interest and confidentiality rules.

1. **Confidentiality**: The external evaluators engaged in the evaluation process are bound to treat all information contained in proposals as strictly confidential. This obligation applies during the evaluation and continues indefinitely after the process has concluded.
2. **Non-disclosure**: The external evaluators must not reveal to any third party the identity of applicants, the content of proposals, or the opinions and assessments of other evaluators, either during the evaluation process or afterwards.
3. **Independence**: Evaluators must not have any involvement in the preparation of proposals submitted to the call and must not benefit, either directly or indirectly, from their selection or rejection.
4. **Conflict of Interest**: Evaluators are required to declare any potential conflict of interest immediately. If such a conflict is identified, the evaluator must withdraw from the assessment of the affected proposal(s).

10. Sub-grant Agreement

Within one week of final result notification, the OCMT will contact the successful applicants to begin contract preparation.
The Sub-grant Agreement will be signed between the CYberSynchrony Coordinator and each third party and will include:

- Specific clauses on cascading funding under Horizon Europe,
- Payment conditions and linked deliverables,

- General legal obligations (IPR, audits, etc.).

Sub-granted projects will then enter the roll-out and monitoring phase under the oversight of the project's implementation team. If a selected legal entity fails to submit the required documentation on time, it will be excluded from the CYberSynchrony programme. The sub-grant agreement can be found on the Open call Synchrony website and is available to all applicants.

10.1. Information on which documentation is mandatory to be submitted, and which should be taken into consideration

Each proposal must include the following mandatory documents at the time of submission. All files must be uploaded via the official CYberSynchrony submission platform before the call deadline.

DOCUMENTATION FOR OPEN CALL APPLICANTS
1. Proposal technical template (MANDATORY) A single PDF file, maximum 10 pages, structured according to the recommended format described in the "Proposal Structure" section. It must include the core technical, implementation, and impact content. The template is provided HERE.
2. Annex 2 - Declaration of Honour SME form (MANDATORY) For monobeneficiary (single entity) proposals, the applicant must be an SME, and the form is mandatory. For consortia of 2 or 3, an SME must be the coordinator of the consortium, and a Declaration of Honour SME form must be filled in and submitted throughout the submission platform. If the consortium has additional SME partners (apart from the SME which will act as the coordinator), the form must be completed by them too. The template is provided HERE.
3. Annex 3 - SME Self-Declaration Form *(MANDATORY)* For monobeneficiary (single entity) proposals, the applicant must be an SME, and the form is mandatory. For consortia of 2 or 3, an SME must be the coordinator of the consortium, and an SME Self-Declaration form must be filled in and submitted throughout the submission process. If the consortium has additional SME partners (apart from the SME which will act as the coordinator), the form must be completed by them too. The template is provided HERE.
4. Annex 5 - Open Call Declaration of Honour - consortium agreement (MANDATORY - ONLY FOR CONSORTIA) For collaborative proposals involving more than one entity, a signed statement confirming joint participation, role allocation, and lead partner must be included. The lead partner must be an SME. The template is provided HERE.
5. ONLY FOR OPEN CALL 3 - MANDATORY REPRESENATION/AFFILIATION LETTER (FOR OPEN CALLS 1 and 2, this document is not required): The coordinator of the consortium must be an SME and is mandatory to provide a letter that proves that the SME represents or is affiliated with a Member State's government, relevant cybersecurity agency, or a recognized research institution. The letter must be signed by both sides. There is no specific template for this letter, applicants should provide their own format, ensuring the above condition.
6. Letters of Support *(Optional)* Applicants may attach letters of support or intent from relevant stakeholders, especially if their proposal includes cooperation with national cybersecurity agencies, sector operators, or Member State institutions. These are not scored but may support the credibility of the implementation. Up to 3 letters of support can be submitted through the submission platform if applicants believe that this is necessary and assists with their content proposition.
7. CYberSynchrony Sub-grant agreement for FSTP (Read only, not required to be submitted at this stage). FSTP applicants are advised to read through the agreement, to clarify questions that may have and concern legal and contractual obligations and terms. This agreement will be signed only by the successful applicants.

DOCUMENTATION FOR EXTERNAL EVALUATORS
1. **Annex A - Open Call contract for external evaluator (Read only, not required to be submitted at this stage)** This is the contract that has to be signed only by the external evaluators who will be selected to review the FSTP proposals. All external evaluators are advised to read through the contract to clarify questions that may have and concern legal and contractual obligations and terms.
2. **Annex B - Conflict of Interest (Read only, not required to be submitted at this stage)** This document contains the terms and conditions related to any conflict of interest related to the proposals that external evaluators will evaluate.
3. **Annex C - Bank details (Not required to be submitted at this stage)** After the selection process, all successful external evaluators should provide their bank details to get the payments according to the number of proposals evaluated.

11. Core CYberSynchrony Modules

The applicants have to ensure that their proposals are strictly aligned with the CYberSynchrony objectives (see section 2 – each Open Call refers to different CYberSynchrony objectives) and Open Call description/KPis (see also section 2). Their proposed work must involve the use of one or more of the CYberSynchrony modules: These modules constitute the technical foundation of the project and represent the operational areas where third-party technologies must connect, integrate, or extend functionality. Each module addresses a specific dimension of cybersecurity preparedness, detection, response, and compliance across national and sectoral environments. Below, there is more information regarding each CYberSynchrony module, however more detailed information concerning our modules can be found in our public deliverables (see section 12).

11.1. CYRESCUE – Resilience and Incident Response

This module acts as the incident response and resilience orchestration layer, coordinating detection results, automating countermeasures, and preserving digital evidence for forensic and legal verification. In addition, the module includes Cyber Security Posture Assessment (CSPA), Purple Team Assessment (PTA), and Security Breach Simulation (SBS) to test operational readiness, validate incident response playbooks, and quantify resilience improvements over time.

List of tools included in CYRESCUE:

1. Cyber Security Posture Assessment (CSPA)
2. Purple Team Assessment (PTA)
3. Security Breach Simulation (SBS)

CSPA – Cyber Security Posture Assessment (more info in D3.2, section 12):

- Web-based dashboard for assessing organizational maturity and compliance posture.
- REST API for automated submission of system metrics and retrieval of posture scores.
- Export capability in JSON and CSV for integration with compliance reporting tools.

PTA – Purple Team Assessment (more info in D3.2, section 12):

- Controlled environment for conducting coordinated Red/Blue team exercises.
- Provides simulation templates (attack scenarios, MITRE ATT&CK mappings).
- Results accessible via secure API or downloadable JSON reports.

SBS – Security Breach Simulation (not included in a deliverable yet):

- Cloud-deployable engine for executing controlled breach and ransomware simulations.
- Configurable scenarios via web dashboard or API endpoints.
- Generates forensic data and reports for analysis within the CYRESCUE environment.

- Campaigns with Caldera (SBS uses MITRE Caldera to conduct realistic, campaign-style red team simulations within dockerised environments. These simulated attacks reproduce various threat actor behaviours and test the organisation's detection and response mechanisms. SBS provides a visual and interactive way to assess readiness against evolving adversary tactics through discovery and attack lifecycle emulation).

Which are the general requirements for the tools/solutions that will be developed for CYRESCUE Integration:

- Strict adherence to data formats such as JSON, STIX 2.1, and TAXII, for structured threat intelligence sharing.
- A sandbox environment with mock data is available to selected applicants for testing.

11.2. CYBERRA – Threat Intelligence and Risk Analysis

CYBERRA enables Member States and critical infrastructures to understand, anticipate, and mitigate evolving cyber threats through real-time intelligence and data-driven risk assessment. It provides continuous threat monitoring, vulnerability correlation, and contextual risk analysis tailored to national or sectoral environments. The module aggregates global threat intelligence, correlates Indicators of Compromise (IoCs) with local events, and models customized risk scenarios to identify high-impact vulnerabilities before they are exploited. It also supports the execution of controlled attack simulations and security posture evaluations to strengthen organizational readiness. In addition, CYBERRA supports operational decision-making through **Defensive Cyber Operations (DCO)** playbooks, which translate threat intelligence findings into structured response actions. These playbooks assist security teams in evaluating response options, understanding potential impact, and preparing coordinated mitigation actions before threats materialise into incidents. All threat intelligence data and analytical outputs are stored and processed with verifiable forensic integrity, ensuring that information remains reliable, traceable, and tamper-resistant. CYBERRA integrates MISP as its core threat intelligence platform and provides the analytical foundation that informs downstream modules responsible for incident response coordination and resilience assessment.

List of tools included in CYBERRA:

1. MISP
2. Defensive Cyber Operations/Response Playbooks (DCO)

MISP – Threat Intelligence Platform (more info in D3.1 – see section 12):

- Web-based interface for viewing and managing Indicators of Compromise (IoCs).
- REST API for automated ingestion and export of threat data in STIX/TAXII or JSON format.
- Supports authentication via API keys and HTTPS/TLS for secure communication.

DCO (Response Playbooks (more info in D4.2 - D4.4, section 12):

- Playbooks are pre-defined, step-by-step guides that outline responses to specific cybersecurity incidents.

Which are the general requirements for the tools/solutions that will be developed for CYBERRA Integration:

- Strict adherence to data formats such as JSON, STIX 2.1, and TAXII, for structured threat intelligence sharing.
- Organisations can run MISP on its own server or VM (PHP/MySQL stack), collect Indicators of Compromise (IoCs) manually or via feeds (STIX/TAXII), and export IoCs in multiple formats (JSON, CSV, XML) or expose them via its REST API.
- A sandbox environment with mock data is available to selected applicants for testing.

11.3. CYBRITE – Continuous Monitoring and Early Threat Detection

CYBRITE focuses on enabling real-time monitoring of cyber threats and the rapid detection of anomalies before they escalate into full-scale incidents. It forms the core detection and monitoring layer of the CYberSynchrony ecosystem, integrating host-based, network-based, and behavioural analytics tools. Through the combined use of Security Information and Event Management (SIEM) technologies (e.g., Wazuh), network intrusion detection systems (e.g., Suricata), and machine-learning-based anomaly analysis (Anomaly Detector IDS and WEKA), the module provides full visibility over infrastructure and user activity. The combination of these multiple data sources enables CYBRITE to achieve early threat detection, proactive risk identification, and timely responses to evolving cybersecurity incidents.

List of tools included in CYBRITE:

Wazuh – Security Information and Event Management (SIEM) (More info in D4.1, section 12):

- Centralised monitoring and alerting interface for endpoints, servers, and applications.
- Collects security event logs via deployed agents and integrates Sysmon telemetry.
- Accessible through the Wazuh Dashboard (HTTPS) and REST API for automation.

Suricata – Network Intrusion Detection and Analysis (More info in D4.1, section 12):

- Inspects live network traffic for suspicious or malicious activity.
- Applies open rule sets (Emerging Threats, custom IDS signatures).
- Outputs JSON-formatted logs (EVE format) compatible with Wazuh's indexer.
- REST API (via Elastic/OpenSearch) for querying and correlation.

Anomaly Detector IDS – Behavioural Anomaly Detection (More info in D4.1, section 12):

- Cloud-based AI/ML engine analysing aggregated Wazuh and Suricata logs.
- Detects abnormal system, network, or user behaviour compared to baselines.
- Provides alert scoring and classification (critical/high/medium/low).
- Exposes REST endpoints for retrieving anomaly reports (JSON).

WEKA – Machine Learning Analytics Engine (More info in D4.1, section 12):

- Supports data-driven pattern discovery and predictive threat analysis.
- Consumes normalised datasets exported from Wazuh and Suricata pipelines.
- Used for UEBA (User and Entity Behaviour Analytics) to detect insider threats.
- Accessible through API for automated retraining and model testing.

Technical Integration Requirements:

- Logs must follow ECS (Elastic Common Schema) and EVE JSON structures for SIEM and IDS compatibility
- Integration with anomaly detection tools (WEKA, AI classifiers) is recommended for behavioural analysis
- Applicants must demonstrate support for cross-system log correlation and real-time alerting.

11.4. CROSS-CORE – Cross-Border Coordination and Secure Information Exchange

CROSS-CORE enables secure collaboration and evidence exchange between Member States, national CERTs, and critical infrastructure operators during cross-border cybersecurity incidents. It ensures that alerts, forensic data, and incident packages can be shared safely, verified for authenticity, and used as trusted evidence in coordinated investigations. The module's architecture combines a Secure Data Exchange Platform with blockchain-based integrity verification, establishing a tamper-proof chain of custody for every exchanged dataset. Through these mechanisms, CROSS-CORE promotes transparency, accountability, and non-repudiation in multi-country operations. It also enforces compliance with European cybersecurity regulations (GDPR, NIS2) by guaranteeing that all shared data follows standardized evidence handling formats and privacy-preserving protocols. In addition to integrity verification and secure transmission, CROSS-CORE supports privacy-aware analytical workflows through

the combined use of Differential Privacy and Homomorphic Encryption. Differential Privacy is applied during dataset processing to limit inference risks, while Homomorphic Encryption enables authorized entities to perform computations directly on encrypted data. These mechanisms complement blockchain-based integrity verification, strengthening trust and accountability in cross-border information exchange without exposing underlying datasets. This module comprises one tool called ***Blockchain integrity validator and more information can be found in D5.1, section 12***.

Technical Integration Requirements:

- Solutions must integrate with the Secure Data Exchange Platform via REST APIs, using:
  - JSON Web Tokens for API authentication
- Data integrity is ensured through SHA-256 hashing and blockchain anchoring
- Supports privacy-aware analytical exchange by integrating Differential Privacy during dataset processing, reducing the risk of attribute inference while maintaining analytical relevance.
- Enables encrypted collaborative analytics through Homomorphic Encryption, allowing computations on protected datasets while ensuring that intermediate components never access plaintext information.
- Data Integrity and Encryption Hyperledger
  - Ensures the authenticity and immutability of all incident data and forensic evidence shared across Member States.
  - Applies SHA-256 hashing and blockchain anchoring to create tamper-proof audit trails.
  - Manages encryption of data in transit and at rest, maintaining confidentiality during exchange.
  - Supports secure data transfer between national SOCs/CSIRTs through JWT-authenticated sessions.

11.5. CYBERWISE – Cybersecurity Awareness and Behavioural Training

CYBERWISE addresses the human dimension of cybersecurity by promoting education, behavioural change, and social resilience against common threats. It combines gamified training modules, interactive awareness platforms, and behavioural analytics tools to engage users across different sectors and levels of expertise. The module also includes capabilities for simulating social engineering attacks, allowing organisations to measure user responses and adapt their awareness strategies accordingly. It also includes behavioural and human risk assessment mechanisms (HRM) that help correlate technical alerts with user-level insights, creating a unified picture of both machine and human threat vectors. Through these mechanisms, CYBERWISE aims to build a culture of security-conscious behaviour that complements technical defences and reduces the likelihood of successful attacks.

List of tools included in CYBERWISE:

HRM - Human Risk Management (more info in D4.1, see section 12)

- Evaluates employee awareness levels, behavioural risk factors, and compliance with cybersecurity policies.
- Generates dynamic risk scores for individuals and departments, highlighting human-related vulnerabilities.
- Integrates with the platform to visualize awareness trends and improvement over time.

Phishing & Social-Engineering Campaigns

- Runs configurable phishing/social-engineering exercises (templates, targeting, scheduling).
- Captures metrics: deliver/open/click/submit/report, and time-to-report.

Cyber-Gate: Gamified Awareness and Training (not included in a deliverable yet)

- Interactive, game-based learning environment that teaches cybersecurity concepts using MITRE ATT&CK tactics and real-world attack paths.
- Users play through simulated cyber incidents, learning how attackers operate and how to defend systems.

- Includes missions, minigames, and progress scoring to engage users while reinforcing secure behaviour.

11.6. CYBERGOPLUS – Governance, Standards, and Regulatory Compliance

CYBERGOPLUS provides tools and environments that help organisations align with European cybersecurity regulations, standards, and certification frameworks. It enables entities to define and enforce internal security policies, monitor compliance across systems and departments, and conduct structured audits. The module incorporates vulnerability management and policy enforcement mechanisms to ensure continuous alignment with NIS2, GDPR, and ISO 27001 requirements. By integrating attack surface visibility (ASA), code-level vulnerability scanning (Snyk), and centralized policy control, CYBERGOPLUS creates a unified compliance layer that bridges technical and organisational cybersecurity governance. This module ultimately strengthens accountability, simplifies regulatory reporting, and promotes harmonisation of compliance practices across sectors and Member States.

List of tools included in CYBERGOPLUS:

ASA – Attack Surface Assessment (more info in D3.2, see section 12)

- Scans infrastructure and endpoints to identify exposed assets, open ports, and misconfigurations.
- Maps discovered assets to vulnerabilities (CVE, CWE, ATT&CK) and provides prioritised remediation guidance.
- Outputs reports for compliance and risk benchmarking against NIS2 or internal standards.

Snyk – Code and Dependency Vulnerability Scanner (not included in a deliverable yet)

- Scans source code, containers, and dependencies for known security flaws.
- Provides developers and auditors with prioritised vulnerability data and recommended fixes.
- Integrates with CI/CD pipelines and exports structured results (JSON) for governance dashboards.

Policy Tools – Compliance and Governance Frameworks

- Enforcement and monitoring of internal cybersecurity policies, track policy adherence
- Map technical controls to compliance frameworks (NIS2, GDPR, ISO 27001).

12. Access to CYberSynchrony Public Deliverables

Applicants interested in submitting proposals under the CYberSynchrony FSTP Open Calls are strongly encouraged to consult the project's public deliverables (Table 8). These documents provide essential technical, architectural, and functional information about the CYberSynchrony ecosystem, which is critical for preparing targeted, high-quality proposals aligned with the project. The deliverables in the green rows in Table 8 are related to the modules of CYberSynchrony whilst the deliverables in the orange rows describe specific aspects of the framework and architecture of CYberSynchrony project. The project consortium has made (and will make in the future) all public deliverables available on the CYberSynchrony project website (link) as they pass through the official approval and publication process. The Open call applicants are strongly advised to consult all deliverables listed in Table 8, to understand technical specifications, architectural principles, and integration expectations relevant to their proposal.

Access to non-public, technical implementation details (e.g., API documentation, sandbox access) will only be granted to successful applicants during the sub-grant agreement preparation phase.

Table 8 CYberSynchrony public deliverables related to the Open Calls

Deliverable Title	Deliverable no.	Access Links (PDF files)
Cybersecurity landscape and threat analysis, end-user requirement analysis, use case definition, and CYberSynchrony Framework – Final version	D2.2	Link
Enhanced Threat Intelligence System v1	D3.1	Link
Risk Scenario Analysis Toolkit v1	D3.2	Link
Integrated Cybersecurity Monitoring Suite v1	D4.1	Link
Automated Response Toolkit v1	D4.2	Link
Secure Data Exchange Platform v1	D5.1	Link
Evidence Integrity System v1	D5.2	Link
CYberSynchrony Integration Blueprint & Use Case Portfolio v1	D8.1	Link