Horizon 2020 Program
ICT-02-2020
Building blocks for resilience in evolving ICT systems

Certifying the Security and Resilience of Supply Chain Services

CYRENE Open Call
Guidelines for Applicants

Table of Contents

Table of Figures

Table of Tables

1. Introduction

This document is the Guidelines for Applicants for the CYRENE Open Call. It provides information and rules for participation to the open call, as well as the funding and schedule scheme.

1.1. Motivation

Global Supply Chain Services (SCSs) underlie the operations of modern businesses, where diverse stakeholders collaborate through complex processes to supply goods to customers. Information and Communication Infrastructures typically support the operation and interactions of the supply chain stakeholders. The Critical ICT Infrastructures are subject to threats as the underlying assets on which their operation depends have vulnerabilities that can be exploited either through malicious attackers of unintentionally.

Although cybersecurity tools and products for handling threats have greatly evolved, there is still no easy, structured, standardized and trusted way to forecast, prevent and manage interrelated and propagated cybersecurity vulnerabilities and threats. Thus, there is a pressing need for devising methodologies, techniques and tools for the efficient evaluation and handling of security threats and vulnerabilities in Supply Chain environments.

1.2. CYRENE Overview

CYRENE is a European project, funded under the Horizon 2020 Work Programme under contract number 952690. It focuses on the development of novel solutions for enhancing control, handling security threats and vulnerabilities and ensuring accountability of ICT systems, components, and services across the supply chains. These issues are addressed via a dual-use methodology, the Risk and Conformity Assessment (RCA) Methodology, and a set of tools that support this methodology. These tools assess the security and the resilience of Supply Chain Services, the interconnected ICT infrastructures supporting these services and the assets that support the operations of the Supply Chains.

1.3. CYRENE Platform

The CYRENE Platform comprises a set of tools that support the defined RCA methodology. It follows a layered and modular approach, which aims at ensuring security-by-design, interoperability and continuous evolvement among all the components. Figure 1 depicts the conceptual CYRENE Architecture diagram including the main components, information flows and API interactions among them. The architecture puts emphasis on the way pipelining of information, i.e., user authentication, secure services certification, data management on five (5) vertical cybersecurity layers of services, the collaborative risk assessment, and the visualisation layer, is safeguarded ensuring smooth interoperation of the underlying services. As shown in Figure 1, the CYRENE framework is based on different Cybersecurity Layers. The Protection and Regulation Layer ensures Confidentiality, Integrity, Availability (CIA) and mechanisms that are enforced in the Security Layer, which acts horizontally for the entire CYRENE Platform. As depicted in the figure, V1-V4 generate analytics, reports and alerts, which are stored in the Data Management Layer and are further populated in the Visualisation Layer. The Data Management Layer provides all the modalities to exchange and interface data through message queues, relational and schema-less structures. Besides, H1-H3 that support the Collaborative Risk Assessment of SCS gets input from the Dynamic Vulnerability Assessment Layer for assessing the identified vulnerabilities according to the Common Vulnerability Scoring System (CVSS 3.1)[1].

[1] https://www.first.org/cvss/calculator/3.1

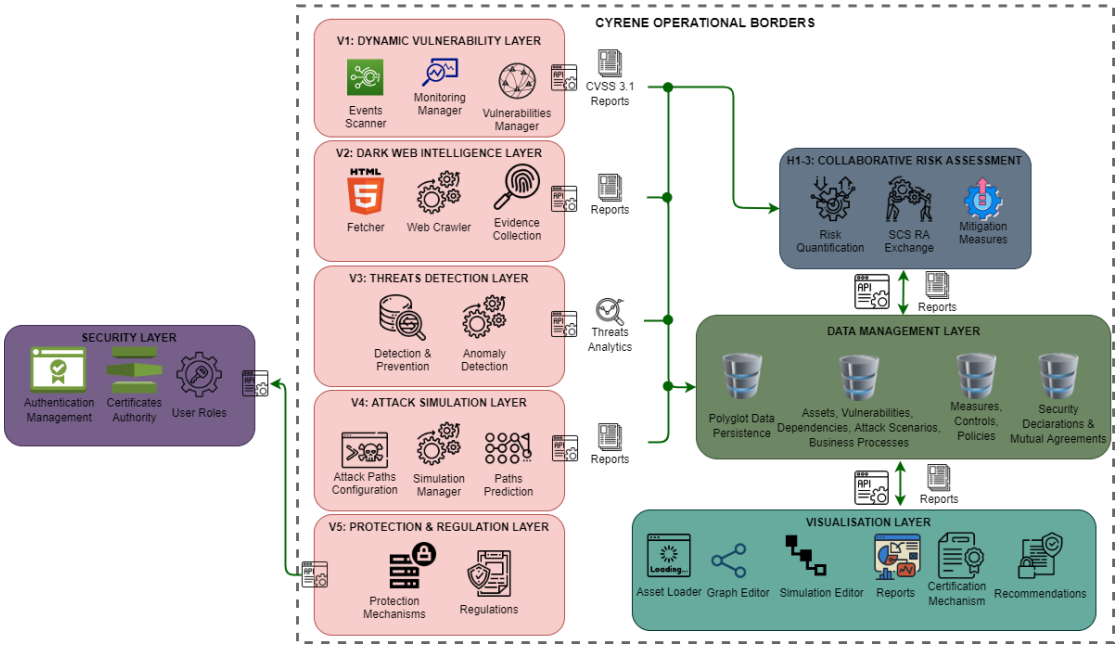

Figure 1. CYRENE Conceptual Architecture.

The functionalities of the CYRENE Platform and its interactions with the core CYRENE actors are shown in Figure 2.The Use Case Diagram depicts the targeted users of the CYRENE Platform and they ways they interact with it. Different roles have been identified and modelled in the diagram, i.e., the SCS Provider, the SCS Business Partner and the Assessor. The CYRENE Platform that supports the dual use RCA methodology may be used by both the SCS Providers and Business Partners to manage their cyber risks and generate the SCS Protection Profile, and also by third party assessors and certification bodies to assess the SCS Protection Profile (SCS-PP) claims of a Supply Chain Service, generate the audit report and issue a SCS Certificate.

Users with the role of SCS Provider or SCS Business Partner can describe their Target of Evaluation (TOE) by defining security objectives and requirements, business processes, assets and their interdependencies, vulnerabilities and implemented controls. All these are required, along with the definition of business processes and sectorial specificities, to enable the execution of collaborative risk assessment, vulnerability assessment and threat detection services for their supply chain services. Therefore, the SCS Provider or SCS Business Partner can follow the steps of the RCA Methodology and get insights on their risks at any desired Assurance Level (i.e., Basic, Substantial and High).

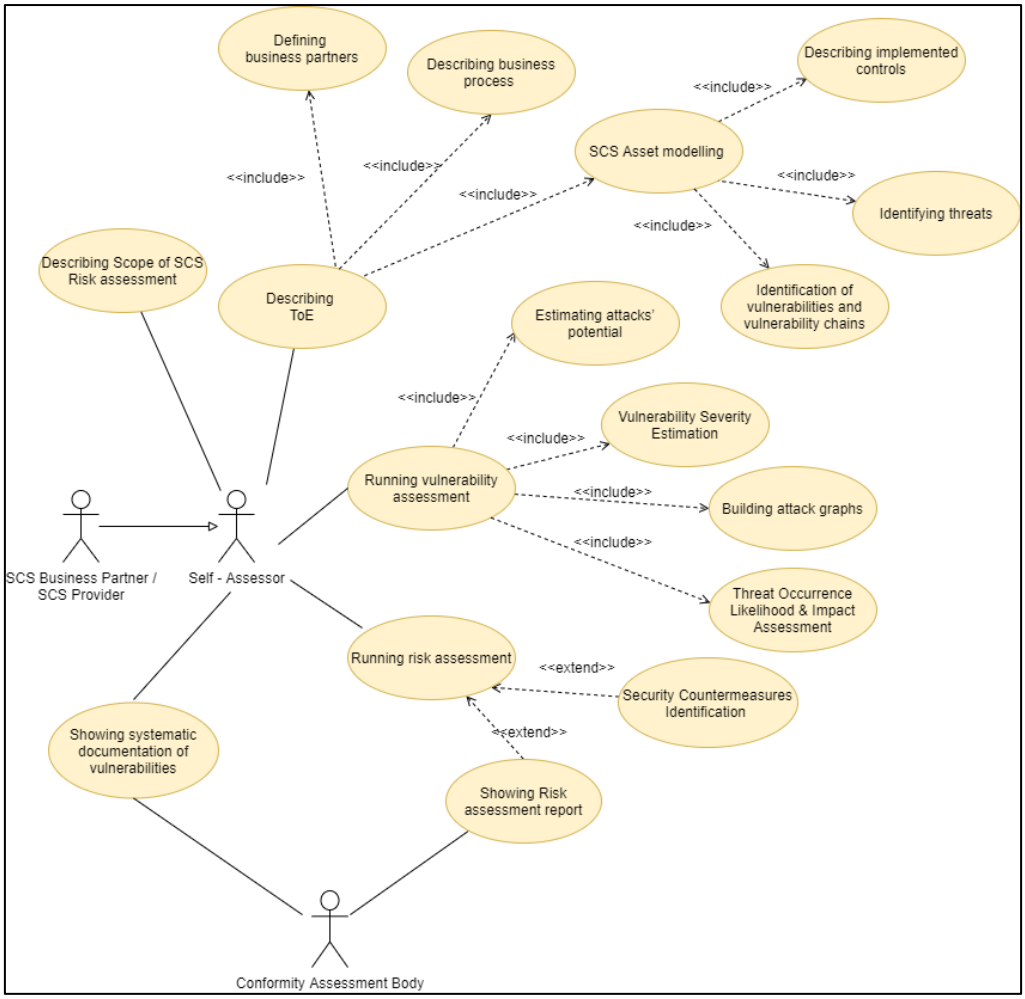

Figure 2. CYRENE Platform Use Case Diagram.

The Assessor role represents users, who use the CYRENE Platform to generate the audit report and issue a SCS Certificate for the supply chain to be assessed. These users are responsible for collecting relevant evidence needed for the assessment of security conformity of a target supply chain. They access systematic documentation of vulnerabilities and obtain risk assessment reports. The Assessor can be a Self-Assessor in case of performing an internal audit for his own SCS of "Basic" Assurance Level without the capability to issue a Certificate. Moreover, the Assessor can be an independent / third party auditor or certification body acting as a Conformity Assessment Body (CAB), who gets access to documented vulnerabilities and risk reports and can perform assessment at any Assurance Level (i.e., Basic, Substantial and High) and issue a certificate for that assurance level.

Aligned with the activities performed by the CYRENE actors, the conceptual architecture of CYRENE Platform aims to support all the steps of the RCA Methodology. The Visualisation Layer and Administration Dashboard assembles all the envisioned components, which allow initiation of the methodology and acquiring insights from the reports, analytics, and alerts for the supply chain component. The Data Management Layer supports all the data modalities and the knowledge bases for integrating heterogeneous data with different attributes, i.e., from assets, business processes and assets dependencies, to evidence collection, vulnerabilities quantification and prioritization. It also supports the data, documents and predefined forms for the establishment of Security Declarations and Mutual Agreements. The Collaborative Risk Assessment Layer provides the methods to calculate the risk at individual, propagated and cumulative level of the assets graph specified in a semi-automatic manner through the Asset Loader. Vulnerabilities assessment, evidence-based cyber-intelligence,

threats identification, attack simulations and likelihood calculation are supported by a collection of vertical layers which are the Dynamic Vulnerability Assessment Layer, Dark Web Intelligence Layer, Threats Detection Layer, and Attack Behaviour Simulation Layer. Finally, the Security Layer serves the CYRENE Platform horizontally taking into account policies (e.g., database encryption, setting up of secure communication, etc.) coming from the Protection and Regulation Layer that are enforced by the respective mechanisms. It also supports a Certificate Authority (CA), a User Authorization and Authentication (UAA) service and a Security Configurations Assessment (SCA) module for securing the platform itself under the security-by-design principle.

2. CYRENE Open Call

CYRENE organizes an Open Call during the third year of its lifetime for validating the technologies it has developed in new supply chain domains, and developing new tools that, when integrated to the CYRENE platform, will enhance its functionalities. This chapter gives the details of the objectives, scope and rules of participation to the Open Call.

2.1. Objectives

CYRENE seeks to attract interested candidates to either propose new tools and cybersecurity services by which the CYRENE platform may be enriched or evaluate the platform in other vertical supply chain domains. Proposals to the Open Call may address:

- Development of software for a new product / service that can be integrated to the CYRENE platform, or
- Evaluation of a use case coming from new vertical domains, e.g., Healthcare, FinTech, Manufacturing, Agrifood, E-Government, Retails, Construction, Logistics, Education, etc.

In particular, the CYRENE Consortium seeks:

- Cybersecurity Vendors or Cybersecurity Service, Product, Application Providers to introduce tools and/or services and thus enrich the current CYRENE portfolio of tools and services. The new tools and services must solely rely on Open-Source software solutions.
- Use Case applicants operating in domains including but not limited to Healthcare, FinTech, Manufacturing, Agrifood, E-Government, Retails, Construction, Logistics, Education with established supply chains and collaborations with third party services to assess the CYRENE Platform and increase awareness of it.

The CYRENE Open Call will award successful applicants with a grant of up to **€35.000 brutto** for *implementing*, *integrating and testing new cybersecurity tools and services* to the CYRENE Platform and with a grant of up to **€8.000 brutto** for defining *new use cases from different vertical domains* in order to validate the CYRENE Platform in these domains. The Open Call will assist in the uptake of the existing CYRENE functionalities, the enrichment of the current CYRENE services portfolio and the evaluation of the CYRENE Platform.

2.2. Eligibility and Requirements

The CYRENE Open Call is addressed to Small or Medium Enterprises (SMEs) as they are defined in the EU regulation (EC recommendation 2003/361/EC as published in the Official Journal of the European Union L 124, p. 36 of 20 May 2003). All SMEs eligible for Horizon 2020 are eligible to participate to the CYRENE Open Call except for SMEs that are partners of the CYRENE consortium and parties that may have conflicts of interest with the project. No consortia are eligible for participation.

Moreover, the following requirements must be met by all applicants.

1. Requirements following European directions.
   - Proposals will only be accepted from applicants that are eligible for participation in European projects as defined above.
   - Proposals must have a clear European dimension facilitating innovations in cybersecurity and various industry verticals, contributing towards EU digitization, and targeting clear economic and societal impact.
2. Requirements for Cybersecurity Vendors and Use Cases Applicants.
   - The applicant should be an SME, or Start-up, with a technology developer, and/or integrator, and/or Use Case provider profile, from industries in the areas such as Healthcare, FinTech, Manufacturing, Agrifood, E-Government, Retails, Construction, Logistics, and Education.
   - Participating entities should not have been convicted for fraudulent behaviours, other financial irregularities, unethical or illegal business practices.
   - Applicants are required to submit their proposal online and prepare a proposal according to the provided Proposal Template that accompanies the Open Call.
   - Applicants must accept the terms and conditions and submit the required information of the Open Call.
   - Only one proposal per given organization can be selected for funding in the CYRENE Open Call.
   - Applicants must not have any actual or/and potential conflict of interest with the CYRENE Open Call process, be members of the CYRENE Consortium.
   - Proven competency and experience with Angular 2[2] or greater will be considered as a plus for Cybersecurity Vendors.
3. Additional requirements.
   - The content of a proposal should meet the objectives of the CYRENE Open Call.
   - All proposals must be submitted in the English language.
   - Proposals must address the domain of Cybersecurity, vertical industries in areas including Healthcare, FinTech, Manufacturing, Agrifood, E-Government, Retails, Construction, Logistics, Education, and more, and clearly propose an innovative solution.
   - Applications must only be submitted through the CYRENE Open Call web page, by the deadline.
   - Applications must use the Proposal Template that is available through the CYRENE Open Call web page.
   - The required documents in all phases of the project must be submitted electronically in PDF format without restrictions for printing.
   - All deliverables should be submitted 10 working days before the end of each Stage, see Stage 1 – Stage 4.

2.3. Funding schemes

The CYRENE Open Call foresees two types of funding.

- **Funding of up to €35.000 brutto for new tools and services to be integrated to the CYRENE platform.** Applicants are expected to propose and deliver new tools and services based on Open-Source software, which will enrich the current CYRENE's tool portfolio. The eligible services are the following.
  - Data interoperability services to exchange threats, vulnerabilities and incidents data with open threat sharing repositories (e.g., compliant with

[2] https://angular.io/

OpenCTI[3], STIX[4], MISP[5] and more). To build the schema for this solution, the awarded applicant will need to adhere as closely as feasible to the official STIX v2.1 specification[6]. The final schema will need to, at least, incorporate the following STIX objects
    - STIX Domain Object (SDO),
    - STIX Cyber-observable Object (SCO),
    - STIX Meta Objects (SMO).
  - A data enrichment service, which will create the interconnection graph by exploiting data made available by the CYRENE project related with vulnerabilities and threats. NVD[7] and CAPEC[8] data sources are already connected via CVEs, CWEs[9] and attack patterns. Based on the above-mentioned connections along with the descriptions of vulnerabilities, weaknesses and threats, applicants are requested to implement an expert system (by using graph database[10] / algorithms and/or NLP) to discover: (a) new dependencies between the vulnerabilities, weaknesses and threats; and (b) vulnerabilities / threats communities with similar characteristics that could increase attackers' exploitability capabilities. The CYRENE available dataset is accessible via CYRENE Dataset link.
  - Penetration testing.
  - Endpoint Detection and Response (EDR).
  - Security Operation Centre (SOC).
  - Security Information and Event Management (SIEM) as a Service.
  - Data loss prevention software and encryption tools.
  - Vulnerability and patch management tool.
  - Digital forensics.
  - Multi-layer ransomware protection.
  - Predictive threat intelligence.
  - Multi-level log correlation and analysis.
  - Dynamic application security testing (DAST).
- **Funding of up to €8.000 brutto for validating the CYRENE technologies.** Applicants, including vertical industries use case providers are invited to model and relate their digital or supply chain applications, services, assets and operations with the CYRENE Platform and test its ability to meet their cybersecurity and data protection needs. The eligible use case providers are asked to
  - Define Critical Digital Assets of their organisation, model their assets into business processes and link them into interconnected services.
  - Define Attack Paths, perform Risk Assessment and execute simulation scenarios for possible attack paths.
  - Demonstrate their modelling, definitions, risk and simulation reports to the CYRENE Consortium.
  - Prepare reports compiled for user experience, user journey, user acceptance and provide their feedback for the CYRENE platform.

[3] https://www.filigran.io/en/products/opencti/
[4] https://oasis-open.github.io/cti-documentation/stix/intro.html
[5] https://www.misp-project.org/
[6] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
[7] https://nvd.nist.gov/developers/vulnerabilities
[8] https://capec.mitre.org/data/xml/capec_latest.xml
[9] https://cwe.mitre.org/data/xml/cwec_latest.xml.zip
[10] An indicative graph database might be Neo4J. Available at: https://neo4j.com/

2.4. Open Call Key dates

The key dates of the Open Call are as follows.

October 14, 2022	Open Call launch
November 28, 2022	Open Call webinar
December 5, 2022	Open Call Q+A session
December 16, 2022, 17:00 CET	Open Call submission deadline
January 09, 2023	Open Call result evaluation
January 31, 2023	Contract signature
February 1, 2023	Open Call kick-off meeting
April 21, 2023	Open Call mid-term meeting
July 31, 2023	Open Call final project submission
Early September, 2023	Open Call project presentation

The Open Call timeline is depicted in Figure 3.

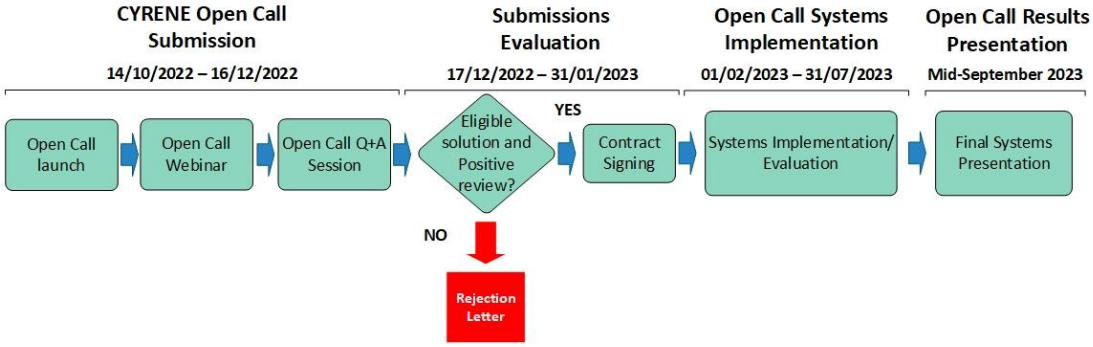

Figure 3: Open Call Timeline.

3. Implementation, Technical Support and Deliverables

The CYRENE Open Call will run for up to six months. This period is broken down to three implementation periods, as shown in the timeline of Figure 3 and detailed in Table 1.

Table 1: CYRENE Open Call implementation timeline.

Timeline	M1 (2/2023)	M2 (3/2023)	M3 (4/2023)	M6 (7/2023)
Meeting	**Open Call Kick-off for funded proposals**	**Conceptualisation, Specifications and Presentation**	**Mid-term Project Review**	**Final Project Review**
Activity	Kick-off presentation: • Work plan description (Timeline, WPs, Tasks, Deliverables). • Objectives of the proposed work / solution. • Key Performance Indicators (KPIs).	Presentation & Report on: • Conceptual Architecture or Definition of Use Cases. • Software Requirements Specification (SRS) or Usage Scenarios for the Use Cases Report.	Presentation & Report on: • Cybersecurity Applicants: a) **First Prototype Demonstration**; and b) **Mid-term Report** (technical report with the early implemented system details, system description, specific API details, i.e., input/output, system integration results and tests (including unit, integration, and acceptance tests). • Use Case Applicants: a) **Use Case Demonstration** in the CYRENE Platform; b) **Mid-term Report** (usage scenarios report with user experience, user journey, user feedback).	Presentation & Final Report on: • Cybersecurity Applicants: a) **Final Product Demonstration**; b) Upload of he developed code to the CYRENE GitLab; and c) **Final Report** (technical report with improvements and delivery details of the final system, system description, specific API details, i.e., input/output, system integration results, unit, functional, integration, and validation tests, cost justification, and recommendations for future improvements). • Use Case Applicants: a) **Final Use Case Demonstration** in the CYRENE Platform; b) **Final Report** (usage scenarios report with user experience, user journey, user feedback, cost justification, and recommendations for future improvements).
Budget Distribution	30%		35%	35%

3.1. Project Implementation Timeline

The project implementation timeline is split into three stages with the corresponding activities and reports that the participants need to fulfil in each of them. The timeline and the corresponding activities are presented into Table 1.

Stage 1 – Open Call Kick-off for funded proposals

The participants will have to present their ideas about how they aim to use the CYRENE framework and how to integrate their work into it. In more detail, the participants need to describe their analytical work plan on specific timeline with clear definition of the WPs, tasks and deliverables. Also, they need to describe their proposed solutions objectives and their Key Performance Indicators (KPIs).

Stage 2 – Project Architecture and Use Cases Conceptualisation, Specifications and Presentation

The participants will have to design and present the Conceptual Architecture of the technical solution in the case of Cybersecurity Applicants. The Use Case Applicants are requested to prepare and define their scenarios, the critical digital assets they bring on board onto the CYRENE project, as well as the current as-is and future to-be use cases and how they envision to be modelled and implemented within the CYRENE Platform.

Stage 3 – Mid-term Project Review

The implementation and the initial results of the implemented components need to be presented in the mid-term review meeting. The Cybersecurity applicants have to provide a detailed technical report about their system first prototype, i.e., input/output info details, system components description, system integration results and validation tests. On the other hand, the Use Case applicants need to present their proposed use case scenarios, their proposed tests and their feedback about the CYRENE framework.

Stage 4 – Final Project Review

The participants will have to present their final results to the CYRENE consortium in a final project report. In more details, they will present all the technical details of the implemented system, i.e., system description, specific API details, i.e., input/output, system integration results, and unit, functional, integration, and validation tests. Also, the report will describe the cost of the implemented systems and the participants recommendations about future improvements of their systems. On the other hand, Use Case applicants will describe their experiences based on specific run scenarios and they will offer their feedback with recommendations for future CYRENE framework improvements.

3.2. CYRENE Responsibilities

The CYRENE consortium will provide:

- Presentation of the CYRENE KPIs to motivate and guide the definition / proposition of the Applicants KPIs.
- Technical support for the deployment and integration of new tools into the CYRENE framework.
- Technical support for the development of the new use cases enriching the CYRENE framework.
- Detailed guidelines for the final system or use cases evaluation.

3.3. Deliverables

Three deliverables must be produced during the implementation phase.

Deliverable 1: At project initialization the funded project should prepare a Report including a Conceptual Architecture or the definition of the Use Cases. This Report should also include the Software Requirements Specification (SRS) regarding the software

development activities or the description of the Usage Scenarios regarding the Use Cases.

Deliverable 2: a Mid-term Report should be prepared and delivered. The *Mid-term Report of the Cybersecurity Applicants* will have to prepare a technical report, where the early implemented system details will be presented. In addition, specific API details, i.e., implemented systems input/output will be presented. Last, the report will collect and describe all the information regarding the experiments and their corresponding system tests and results. The *Mid-term Report of the Use Case Applicants* will present the usage scenarios, user experience and user journey descriptions. Finally, the *Use Case Applicants* have to provide their feedback comments about the CYRENE framework and platform.

Deliverable 3: a Final Report should be prepared and delivered. The *Final Report of the Cybersecurity Applicants* should include technical details about the improvements and the final system, system description, specific API details, i.e., input/output, system integration results, unit, functional, integration, and validation tests, cost justification, and recommendations for future improvements. The *Final Report of the Use Case Applicants* should include description about the final usage scenarios, user experience, user journey, user feedback, cost justification, and recommendations for future improvements.

3.4. Budget Structure

The budget should be presented and justified in Section 3 of the Proposal Template. It should contain the team members, the personnel rate and the estimated time to be allocated in the development phase (either for the software development activities or for the use case development activities). Equipment costs are eligible under detailed justification.

3.5. Budget Distribution

The funds that will be granted to each successful proposal will be distributed as follows:

- 30% upon presentation of the concept of the proposal and specifications of the proposed solution.
- 35% upon successful completion of the mid-term review.
- 35% upon successful completion of and presentation of the project.

3.6. Eligible Costs

The eligible costs are

1. Personnel costs.
2. Equipment costs under detailed justification.

4. Proposal Submission and Evaluation

4.1. Proposal Submission

All proposals should be submitted electronically in a single-stage through the CYRENE Open Call web page. All supporting documentation, including the Proposal Template, is available for download through the CYRENE website.

4.2. Proposal Template

The Proposal Template should be used for preparing a proposal. The template has been designed to ensure that the important aspects of the planned work are presented in a way that will enable the evaluators to make an effective assessment against the evaluation criteria.

The page limit is 12 pages per proposal. All tables, figures and references must be included as an integral part of the document and are thus counted against this page limit. Excess pages (in over-long proposals) will not be taken into consideration by the evaluators.
Evaluators will *ignore hyperlinks* to information that is specifically designed to expand the proposal, thus circumventing the page limit. Only references and links that point to the mandatory proof of maturity of the solution will be accepted.
The following formatting conditions apply: the reference font for the body text is Helvetica. The use of a different font for the body text is not advised and is subjected to the cumulative conditions that the font is legible and that its use does not significantly shorten the representation of the proposal in number of pages compared to using the reference font (for example with a view to bypass the page limit). The minimum font size allowed is 11 points. Standard character spacing and a minimum of single line spacing has to be used. Text elements other than the body text, such as headers, foot/end notes, captions, formulas, may deviate, but must be legible. The page size is A4, and all margins (top, bottom, left, right) should be at least 15 mm.
For keeping the formatting of the document, use of Microsoft Word or Word Online is recommended.

4.3. Evaluation Process

CYRENE will approve and appoint an Evaluation Committee composed of external experts to evaluate the submitted proposals. The submitted proposals will be ranked per category. Financial awards will be given to the highest ranked proposals that can be covered by the CYRENE available funds for the Open Call. The whole process will be supervised and finally approved by the CYRENE Project Steering Committee.
Once the evaluation process is completed, all applicants, whether successful or unsuccessful, will receive a notice on the outcome of the evaluation and their Evaluation Summary Report. The selected applicants will receive an in-detail email with the steps for contract signature.

4.4. Evaluation Criteria

The evaluation of the proposals will be made by an external evaluation committee and will be based on the criteria that are shown in Table 2.

Table 2: CYRENE Open Call proposal evaluation criteria.

Proposal Evaluation	Description
Excellence and Innovation (max 6 pages)	• Motivation & Proposal vision • Technology background • Propose Concept & Technical advantages to the CYRENE platform
Impact (max 2 pages)	• Advantages to Supply Chain security • Set clear and realistic KPIs • Define advantages to CYRENE KPIs • Develop an appropriate dissemination plan for the CYRENE framework and tools.
Implementation (max 4 pages)	• Develop a coherent and clear work plan with specific WPs, Tasks and GANTT • Describe analytically the Deliverables and the corresponding Milestones. • Resources

Each criterion will be evaluated with a score between 0 and 5. The evaluation scores are as follows.

- **0 (fail)**: The proposal fails to address the criterion or cannot be judged due to missing or incomplete information.
- **1 (poor)**: The criterion is addressed in an inadequate manner or there are serious inherent weaknesses.
- **2 (fair)**: The proposal shows significant weaknesses.
- **3 (good)**: The proposal addresses the criterion well even though improvements would be necessary.
- **4 (very good)**: The proposal addresses the criterion very well, although targeted improvements are still possible.
- **5 (excellent)**: The proposal successfully addresses all relevant aspects of the criterion in question.

The passing threshold for each criterion is 3/5. A proposal must score at least 10 points to be considered for fund award.

5. Support

In addition to this Guide for Applicants, the following supporting tools are available:

- Frequently Asked Questions

  A Frequently Asked Questions document about CYRENE framework is available on the website. The document will be periodically updated to reflect the questions received.
- CYRENE newsletter

  Applicants should subscribe to the CYRENE newsletter on the website to be notified about Open Call webinars that will be organized by the project.
- CYRENE Contact

  https://www.cyrene.eu/contact/