CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

CyberSecDome

An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.

CyberSecDome Open Call

General Guide

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

TABLE OF CONTENTS

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

1 Introduction

Digital transformation has brought immense benefits to organisations across sectors, enabling new business models, improved services, and enhanced customer experiences. However, this rapid adoption of digital infrastructures has also introduced significant security challenges. Critical service delivery and business continuity are at constant risk due to evolving cybersecurity threats.

To address these challenges, **CyberSecDome** offers an innovative approach that combines cutting-edge **AI-enabled security tools** and **Virtual Reality (VR)** technologies to enhance the security, privacy, and resilience of complex and heterogeneous digital systems. The project focuses on providing **real-time threat detection, incident management, and dynamic response** capabilities optimised through collaboration among stakeholders within digital infrastructure ecosystems.

The overall objective of CyberSecDome is to democratise AI and VR technologies to:

- **Predict cybersecurity threats** and associated risks.
- **Dynamically manage incidents** by providing AI-optimized responses.
- **Facilitate collaboration** and knowledge-sharing among stakeholders through privacy-aware mechanisms.
- **Improve situational awareness** using immersive VR tools, allowing stakeholders to monitor threats and responses in real-time.

Through the **CyberSecDome Open Call**, the project invites SMEs, Industries, and other stakeholders across Europe to participate in testing and further developing these technologies. The Open Call provides a unique opportunity to extend the application of CyberSecDome's solutions to real-world use cases, ensuring their practical relevance and contributing to the overall security of Europe's digital infrastructures.

2 CyberSecDome Open Call Overview

2.1 What is CyberSecDome?

CyberSecDome is a project designed to address the ever-growing cybersecurity threats faced by organisations and digital infrastructures across Europe. The project leverages the power of **Artificial Intelligence (AI)** and **Virtual Reality (VR)** to create advanced security frameworks that provide real-time threat detection, incident management, and collaborative responses.

The project's unique feature lies in its integration of VR technology, which enhances situational awareness by immersing stakeholders in a visual and interactive environment. This allows for real-time monitoring of detected incidents, ongoing risks, and the execution of selected responses. In addition to VR, AI-powered tools enable better prediction of cybersecurity risks and automate the incident response process, making CyberSecDome an innovative approach to safeguarding digital infrastructures.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

2.2 Open Call Structure

The CyberSecDome Open Call is structured into two rounds, each aligned with the project's development milestones:

- **Round 1**: Focuses on testing the early-stage CyberSecDome prototype, allowing participants to validate the project's capabilities in controlled environments. This round aims to gather feedback from real-world use cases and improve the system's design for subsequent releases.
- **Round 2**: Targets more advanced use cases, focusing on testing the final prototype in diverse, real-world infrastructures. Participants in this round will play a crucial role in demonstrating the system's effectiveness and contributing to the final refinement before full deployment.

2.3 Funding Details

The total budget for the CyberSecDome Open Call is **€1.2 million**, distributed across the two rounds as follows:

- **Round 1**: A budget of **€420,000** is allocated, with a maximum of **€120,000** per project. Micro, small, and medium-sized enterprises (SMEs[1]) can request up to 100% funding, while larger enterprises (aka industry) may be required to co-fund 50% of the project's cost. Proposals should justify the requested budget based on the scope and complexity of the work.
- **Round 2**: The remaining budget will be allocated based on the outcomes and recommendations from Round 1. Participants in this round will be involved in deploying the more advanced version of the CyberSecDome system.

Table 1. Funding Details for CyberSecDome Open Call

Funding Aspect	Description
Total Budget for Open Call	€1,200,000
Round 1 Budget Allocation	40% of the total budget (€480,000)
Round 2 Budget Allocation	60% of the total budget (€720,000), with any unused funds from Round 1 carried over
Maximum Funding Per Proposal	€120,000
SME Funding Rate	Up to 100% of eligible costs covered
Large Industry Funding Rate	Up to 50% of eligible costs covered
Consortia Funding Rate	SMEs: Up to 100%; Large Industries: Up to 50%

1 https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Grant Payment Schedule	○ 30% following the signing of the agreement (M1) ○ Up to 30% after positive interim assessment (M9) ○ Up to 40% after positive final assessment (M12)
Unused Funds in Round 1	Any unused funds from Round 1 will be added to the Round 2 budget

Contributing additional resources will be viewed favourably in the evaluation process, as it demonstrates the applicant's commitment to the project's success.

3 Who should participate

The **CyberSecDome Open Call** is designed to engage European companies and institutions committed to addressing significant cybersecurity challenges. This includes both **product developers** and **service providers** in the cybersecurity domain, as well as **end-users** of advanced security resources who aim to protect their digital infrastructure from cyber threats.

The Open Call is particularly suited for:

- **Micro, small, and medium-sized enterprises (SMEs)**: Companies developing or using innovative cybersecurity solutions, particularly those looking to integrate AI and VR tools into their security operations.
- **Research institutions**: Organizations specialising in cybersecurity research and innovation, eager to collaborate on testing and refining cutting-edge solutions in real-world scenarios.
- **Public and private sector entities**: Institutions that manage complex digital infrastructures and are interested in enhancing their resilience and security through advanced, AI-driven cybersecurity frameworks.

Applicants should demonstrate a willingness to test and implement **innovative approaches** in cybersecurity, especially solutions that utilise AI and VR for **real-time threat detection, incident management**, and **collaborative responses**. Participation in the Open Call provides the opportunity to work directly with the CyberSecDome consortium, gaining access to cutting-edge technologies and contributing to the future of cybersecurity in Europe.

Eligibility Criteria:

- Applicants must be legally established entities within the **European Union (EU)** or in countries associated with **Horizon Europe**.
- At least one participant in the consortium (if applicable) must be an **SME**.
- Proposals should align with the **CyberSecDome project's objectives** and demonstrate the ability to apply the project's solutions in real-world use cases.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

4 How to participate

Participation in the **CyberSecDome Open Call** requires applicants to submit a detailed proposal through the dedicated submission platform. The following outlines the key steps and guidelines for participation.

4.1 Proposal Submission Guidelines

Applicants must prepare a comprehensive proposal that addresses the specific objectives of the CyberSecDome project. The proposal should include the following sections:

- **Administrative Information**: Basic details about the applicant(s), including organization name, contact information, and legal status.
- **Excellence**: A clear description of the project's objectives and how it aligns with the **CyberSecDome use cases**. This section should highlight the innovative aspects of the proposed solution and its relevance to cybersecurity challenges.
- **Impact**: Applicants should define measurable key performance indicators (KPIs) and demonstrate the potential business and technical impact of their solution. The proposal should also outline plans for sustainability beyond the project's funding period.
- **Implementation**: A detailed work plan should be provided, including timelines, milestones, and risk management strategies. Applicants should describe the technical and human resources required to successfully implement the proposed solution.
- **Budget**: A high-level budget that justifies the requested funding should be included, specifying the allocation of resources and costs across the project's duration. Contributions beyond the requested funding will be positively considered.

4.2 Proposal Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- **Excellence**: Proposals must clearly define the project objectives, addressing specific **cybersecurity challenges** through the innovative application of **AI** and **VR** technologies.
- **Impact**: Proposals should demonstrate the **technical and business impact** of the proposed solution. Clear KPIs and expected outcomes should be provided.
- **Implementation**: Applicants must present a detailed implementation plan, with a clear timeline, well-defined milestones, and appropriate risk mitigation strategies.
- **Alignment with CyberSecDome Objectives**: Proposals should align with the core objectives of CyberSecDome, contributing to the improvement of **digital infrastructure security** through the use of **AI and VR** technologies.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Value for Money**: The proposed budget must be reasonable and well-justified, demonstrating a cost-effective approach to achieving the project's objectives.

Each proposal will be scored on a scale of 0 to 5 for each criterion. The detailed scoring methodology is provided in the **Annex: Evaluation Criteria** section.

4.3 Submission Platform and Process

Proposals must be submitted electronically through the **CyberSecDome Open Call submission platform** by the stated deadline. The platform will guide applicants through the submission process, ensuring all required sections are completed and supporting documentation is uploaded.

Key points to note:

- The submission must be in **English**.
- Proposals that do not meet the submission requirements or exceed word/page limits will be **disqualified**.
- It is highly recommended that applicants initiate contact with the **CyberSecDome consortium** well before the submission deadline to clarify any questions regarding the Open Call guidelines.

4.4 Communication with Open Call Organisers

Applicants can reach out to the CyberSecDome Open Call organisers through the following channels to clarify questions or request further information about the Open Call:

- **Email**:
  - opencall@cybersecdome.eu
  - info@cybersecdome.eu
- **Website**: Visit the CyberSecDome official website at https://cybersecdome.eu/.
- **LinkedIn**: Engage with the project and stay updated on Open Call-related posts via CyberSecDome's LinkedIn page.
- **X (formerly Twitter)**: Follow updates and communicate with the team on CyberSecDome's X account.
- **YouTube**: Access video updates, tutorials, and other resources on CyberSecDome's YouTube channel.
- **Submission Platform**: Use the submission page for inquiries related to proposal submission at https://www.f6s.com/cybersecdome-open-call-round-1.

Applicants are encouraged to reach out early to ensure they receive timely support and clarification for preparing their submissions.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5 Annexes

5.1 Annexe: CyberSecDome Open Call Program Details

The **CyberSecDome Open Call Programme** is part of a broader initiative funded under the **Horizon Europe** framework to enhance the resilience, security, and accountability of digital infrastructures using AI and VR technologies.

5.1.1 Programme Objectives

The main objectives of the CyberSecDome Open Call are:

- **To enhance threat detection and incident response**: By leveraging AI, the programme seeks to develop and validate tools to detect cybersecurity threats in real time, predict potential attacks, and optimise incident responses through automated systems.
- **To promote collaboration and information sharing**: The programme emphasises the importance of cooperation between stakeholders (public and private) in managing cybersecurity risks. Information-sharing platforms developed as part of the project will enable stakeholders to exchange threat intelligence, thereby improving collective resilience.
- **To integrate VR for situational awareness**: Including VR tools in cybersecurity management is a key innovation of CyberSecDome. These tools will allow security teams to visualise threats and incidents in immersive environments, improving real-time decision-making and enhancing response strategies.
- **To test and validate solutions**: The Open Call will support external organisations in testing CyberSecDome's AI-driven and VR-enhanced cybersecurity tools in real-world scenarios. This will help ensure the tools are practical, scalable, and adaptable to various sectors.

The Open Call seeks to attract innovative proposals that align with these objectives and contribute to developing CyberSecDome's advanced security solutions.

5.1.2 CyberSecDome Open Call Rounds

The programme is structured into two rounds of funding to align with CyberSecDome's development milestones:

- **Round 1**: Focuses on testing the early prototype of CyberSecDome and its core functionalities. Selected participants will be able to use and validate early-stage solutions in controlled environments. The feedback participants provide will inform the development of the next iteration of the platform.
- **Round 2**: In this round, the final prototype will be tested in more complex, real-world infrastructures. This phase focuses on demonstrating the full capabilities of the platform, including its AI-driven threat detection and VR-based incident response systems, in diverse operational environments.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5.1.3 Funding and Financial Structure

The **CyberSecDome Open Call** has a total budget of **€1,200,000** allocated across two rounds of project funding:

- **Round 1:** Will receive **40% of the total budget,** amounting to **€480,000**.
- **Round 2:** Will receive **60% of the total budget**, amounting to **€720,000**.

If any funds from **Round 1** remain unallocated, the remaining amount will automatically roll over into the **Round 2** budget, increasing the available funds for **Round 2**.

5.1.3.1 Funding Conditions and Rules

The Open Call Max Contribution for each proposal **is capped at €120,000**, regardless of the total project budget submitted by the applicant. While **SMEs will be funded at 100%** of their eligible costs, and **larger industries will be funded at 50%,** no applicant (whether an SME, larger industry, or consortium) will receive more than **€120,000** for a single proposal.

Applicants are encouraged to propose a budget that reflects the actual cost of executing their project. However, regardless of the total budget proposed**, the Open Call Max Contribution is capped at €120,000** per proposal, for both SMEs and larger industries. **Any costs exceeding this amount must be covered by the applicant**.

For consortium proposals, the €120,000 cap applies to the entire consortium, and applicants must allocate the funding accordingly. It is the responsibility of the consortium members to cover any costs that exceed the maximum Open Call contribution.

5.1.3.2 Example 1 – SME

An SME submits a proposal with a total budget of €150,000. Since the maximum contribution from the Open Call is capped at €120,000, the SME will receive the full €120,000 from the Open Call, and they will need to cover the remaining €30,000 from their own resources.

5.1.3.3 Example 2 – Larger Industry

A larger industry submits a proposal with a total project budget of €300,000. As a larger industry, they are eligible for 50% funding, but the maximum funding they can receive is €120,000, not €150,000, due to the cap. Therefore, the industry will receive €120,000, and they must cover the remaining €180,000 from their own resources.

5.1.3.4 Example 3 – Consortium (1 SME + 1 Larger Industry)

A consortium consisting of one SME and one large industry submits a joint proposal with a total budget of €200,000. The funding will be distributed as follows:

SME:

- The SME contributes 50% of the total budget, which is €100,000.
- Since SMEs are funded at 100% of their eligible costs, the SME will receive €100,000 from the Open Call to cover its entire share of the budget.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Larger Industry:

- The large industry contributes the remaining 50% of the total budget, which is also €100,000.
- As a larger industry, it is eligible for 50% funding, meaning it would normally be eligible to receive €50,000. However, since the Open Call Max Contribution is capped at €120,000, and the SME has already received €100,000, the remaining €20,000 will be allocated to the large industry, instead of the full €50,000 it would otherwise be eligible for.

Remaining Budget:

The large industry will need to cover the remaining €80,000 from its own resources (since its total budget is €100,000 and it only receives €20,000 from the Open Call).

5.1.3.5 Example 4 – Consortium (2 SMEs + 1 Large Industry):

A consortium consisting of two SMEs and one large industry submits a joint proposal with a total budget of €350,000. The funding will be distributed as follows:

SMEs:

- Each SME contributes 33% of the total budget, which is €116,667 per SME.
- Since SMEs are funded at 100% of their eligible costs, both SMEs are eligible to receive full funding for their share, but the total consortium funding is capped at €120,000.
- As the consortium cannot receive more than €120,000, the two SMEs will share a portion of this total.
- Each SME will receive €58,333.50.

Larger Industry:

- Large industry contributes 34% of the total budget, which is €116,666.
- As larger industries are only eligible for 50% funding, this would mean the industry could receive a maximum of €58,333 if there were no cap.
- However, since the total consortium funding is capped at €120,000, the large industry will receive €0, as the total €120,000 will be used to fund the SMEs.

Remaining Budget:

- The remaining budget that exceeds the Open Call funding (i.e., €230,000) will need to be covered by the consortium members themselves, split proportionally:
- Each SME will need to cover an additional €58,333.50 (since they originally proposed €116,667, but only €58,333.50 is funded).
- The large industry will need to cover its full €116,666 share from its own resources.

5.1.3.6 Grant Disbursement Schedule

To ensure smooth funding, grants will be disbursed in the following schedule, tied to key milestones and assessment points within the project timeline:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Table 2. Grant Disbursement Schedule

Grand Percentage	Conditions/ Terms	Expected Period (Project Month)
30%	Following the Agreement's signed by all the Parties	M1

Up to 30%	• Positive Interim Assessment outcome
	• Approval by EIT Digital of the following documentation submitted by the Selected Third Parties:
	  ○ Deliverables (if applicable)
	  ○ Technical Report (Annex 3)
	  ○ Financial Statements (Annex 2)
		M9

Up to 40%	• Positive Final Assessment outcome • Depending on the cumulative eligible costs per Selected Third Party and the max approved Grant amount.	M12

5.1.4 Eligibility and Application Conditions

To ensure a fair and transparent process, the **CyberSecDome Open Call** has clearly defined eligibility criteria and application conditions for all applicants. These criteria ensure that the project remains aligned with the objectives of the **Horizon Europe Programme,** while encouraging the participation of SMEs and other stakeholders across Europe.

To effectively meet all submission requirements, the applicants should consult the CyberSecDome consortium well in advance of their proposal submission while designing and preparing their proposal. It is strongly advised to avoid waiting until the last minute to submit proposals, as this can result in a high volume of requests to the system, potentially causing delays in processing that cannot be resolved once the deadline has passed.

5.1.4.1 Eligible Applicants

The following entities are eligible to apply for the CyberSecDome Open Call:

- **Micro, small, and medium-sized enterprises (SMEs)**: Applicants must comply with the definition of SMEs according to the **European Commission Recommendation 2003/361/EC**[2] and the **SME User Guide**[3].
- **Large enterprises**: Companies that do not fall under the SME classification are also eligible, but with a lower funding rate.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361
[3] https://ec.europa.eu/docsroom/documents/42921

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Research and academic institutions**: Universities and research centers that contribute to the cybersecurity field can participate as partners in a consortium.

Applicants must be legally established in one of the **EU Member States** or in a country associated with the **Horizon Europe Programme** at the time of the Open Call submission deadline. The following countries are eligible for participation:

- **EU Member States,** including their outermost regions[4].
- Associated countries that have a valid association agreement with Horizon Europe[4].

Important Note: Applicants from **the United Kingdom** and **Switzerland** are **not eligible** to apply for the CyberSecDome Open Call due to their non-association with the Horizon Europe Programme in 2023. If an applicant originates from one of these countries, their proposal will be automatically rejected.

5.1.4.2 Consortia Rules

Applicants may apply individually or as part of a consortium. However, certain rules apply to consortia:

- **Consortium size**: Consortia can consist of up to three partners, with at least one being an SME.
- **SME participation**: In every consortium, at least one SME must be involved, and it should be the leading entity.
- **Consortia funding**: SMEs in consortia are eligible for up to **100% funding**, while larger industry partners will receive up to **50%** funding for their eligible costs.

5.1.4.3 Application Limits

To ensure a diverse and fair evaluation process, the following application limits are in place:

- **Application Limits for Round 1**:
    - **Multiple Submissions per Topic**: Applicants (whether applying as a single entity or as part of a consortium) are allowed to submit multiple applications across different topics within Round 1. However, if an applicant selects Topic 1 (Evaluation & Testing of Integrated Prototype), they cannot apply for any other topics within the same round.
    - **One Application per Topic**: An applicant can submit only one proposal per topic. For example, if an applicant applies to Topic 3 (Incident Handling), they cannot submit a second proposal for the same topic.
    - **Eligibility for Multiple Topics**: Applicants can apply to different topics in Round 1. For instance, an applicant may submit separate proposals for

[4] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Topic 2 (Risk Assessment) and Topic 4 (Automation Pen-Testing), as long as they meet the submission criteria for each topic.

These submission limits ensure that each topic receives unique and targeted proposals while allowing applicants to diversify their participation in multiple aspects of the Open Call.

- **Resubmission for Round 2:** Applicants who submitted proposals for **Round 1** but did not receive funding are eligible to reapply for **Round 2**, provided they meet the eligibility criteria, and their proposal addresses the objectives of the second round.

5.1.4.4 Financial Capability Requirements

All **applicants must demonstrate sufficient financial capability** to support the project's implementation and to cover any remaining costs until the funding is received. This applies particularly to larger industries that are only eligible for 50% funding. Financial capability will be assessed based on the applicant's ability to sustain the project beyond the granted funding amount.

In cases where the applicant's financial capability is in question, additional documentation may be requested to ensure that the applicant has the necessary resources to fulfil their commitments under the project.

5.1.4.5 Compliance with EU Funding Rules

Applicants must ensure that their proposal complies with all relevant EU funding rules, including those related to:

- **Double funding**: Applicants must declare that their proposal is not receiving double funding from other EU sources for the same project activities.
- **Conflict of interest**: All applicants must disclose any potential conflicts of interest that could affect the impartiality of the evaluation process.
- **Fraud prevention**: Applicants must declare that they have not been involved in fraudulent activities and must not be under any current investigation or conviction for fraudulent behaviour.

Failure to comply with these requirements may result in disqualification from the Open Call process.

5.1.5 Programme Timeline and Deadlines

The **CyberSecDome Open Call** follows a structured timeline with specific deadlines for each phase:

- **Round 1 Launch**: December 2024
- **Submission Deadline**: February 2025
- **Evaluation Period**: March to April 2025
- **Project Start**: April 2025
- **Round 2 Launch**: September 2025

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Round 2 Submission Deadline**: October 2025
- **Project Completion**: Final projects from both rounds are expected to be completed by November 2026.

Table 3. CyberSecDome OpenCall Time Table

Round	Action	Dates
Round 1	Detailed dates released	Dec 2024
	Submission period	Jan 2025 - Feb 2025
	Selection, contract signature and onboarding	Mar 2025 - Apr 2025
	Project implementation	Apr 2025 - Nov 2025
	Project performance evaluation	Dec 2025
Round 2	Detailed dates released	Aug 2025
	Submission period	Sep 2025 - Oct 2025
	Selection, contract signature and onboarding	Nov 2025 - Dec 2025
	Project implementation	Nov 2025 - Jul 2026
	Project performance evaluation	Aug 2026

These timelines ensure that projects selected for funding have sufficient time to implement their solutions and contribute to the overall goals of CyberSecDome.

5.1.6 Expected Outcomes

- By the end of the Open Call programme, participants are expected to:
  - Contribute to the validation of **AI-powered** threat detection and **VR-based** situational awareness tools.
  - Provide detailed feedback on the effectiveness of the tools in real-world applications.
  - Propose improvements or adjustments to the tools to ensure they are adaptable to a variety of industries and sectors.

The selected projects will play a key role in ensuring that CyberSecDome's solutions are scalable, practical, and aligned with the current and future needs of **European digital infrastructures**.

5.1.7 Project Structure and Phases

Each project funded through the CyberSecDome Open Call will follow a structured approach with three key phases, ensuring that all participants align their activities with the project's objectives:

Table 4. Project Structure and Phases

Phase	Duration (Months)	Description
Design	1	Planning for using, adapting, and integrating CyberSecDome into third-party infrastructures.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Implementation	5	Performing the work required to deploy the CyberSecDome tools.
Demonstration	2	Testing and demonstrating the applications within the use case scenarios.

5.1.8 Proposal Requirements

A strong proposal for the CyberSecDome Open Call should take into consideration the following aspects:

- **Background in the Cybersecurity Area**: A description of the achievements and strengths of the applicant organisation in the cybersecurity domain, highlighting relevant expertise and successful past projects.
- **Problem/Solution**:
  - Clearly define the **CyberSecDome use case challenge** that the proposal aims to address.
  - Explain the method for integrating the CyberSecDome framework with the applicant's infrastructure, as well as the approach for testing and validating the tools and technologies of CyberSecDome.
- **Impact Outlook**:
  - Outline the applicant's capabilities and plans for deploying and extending the CyberSecDome solution after the pilot phase.
  - Highlight how the proposed solution will contribute to long-term cybersecurity improvements.
- **Team**: Detail the experience and expertise of the team members, specifically in cybersecurity and skills that align with **CyberSecDome's capabilities**.
- **Financial capability**:
  - Applicants should be able todemonstrate the financial capacity to support the project's resource needs until the granted funding is received, if requested.
  - Proposals should be designed with a **lean and cost-efficient approach**, using only the resources necessary to achieve the objectives within the specified timeframe.

The Proposal Submission Template provides even more details on what applicants should take under consideration. The CyberSecDome website provides a template for the Third-Party Funding Agreement (TPFA), which the staff will provide upon request.

The detailed process, including the requirements, criteria and evaluation methodology, is presented in Annex B: Process Overview and Annex C: Evaluation Criteria. Formal requirements on KPIs, financial aspects and partnership are presented in Annex D: Costs

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Reporting and Key Performance Indicators (KPIs), while communication and dissemination guidelines are included in Annex E: Communication, Dissemination, and Visibility.

5.2 Annex B: Process Overview

This annex provides a step-by-step guide for applicants, from proposal submission to the final evaluation process. The aim is to ensure that all applicants clearly understand the procedures involved in the CyberSecDome Open Call.

5.2.1 Proposal Submission

All proposals must be submitted through the F6S platform. The F6S platform was selected as the submission platform for CyberSecDome proposals due to its focus on supporting startups, SMEs, and innovators. It provides a user-friendly interface tailored to managing Open Calls, making it an ideal choice for engaging with small and medium-sized enterprises in the cybersecurity domain. The Submission page is accessible via the CyberSecDome project website and at the following link: https://www.f6s.com/cybersecdome-open-call-round-1. Proposals must be submitted by the deadline specified for each round, and it is the applicant's responsibility to ensure that all required sections are completed and submitted in total. It is also the applicant's responsibility to obtain full commitment and consent from its organisation prior to submission.

- **Submission Deadlines**: Deadlines for each round will be announced and strictly enforced. Late submissions will not be considered under any circumstances.
- **Language**: Proposals must be written in **English**.
- **Format**: Proposals must follow the format and structure outlined in the submission form, with page and word limits strictly adhered to.

5.2.1.1 Steps for Proposal Submission:

- **Step 1 - Platform Access**: Applicants can submit proposals directly via the F6S platform. Registration on F6S is optional but highly recommended, as it facilitates the process by allowing access to updates on the application's progress and streamlined form completion. Registration is free.
- **Step 2 - Completion of Proposal Form**: Applicants must fill in all sections of the proposal form provided on the platform, ensuring all required fields are completed. The form will guide applicants to attach any required documents, as outlined in Annex 5.1.8 and detailed in the Proposal Submission Guideline.
- **Step 3 - Final Review and Compliance Check**: Before submission, applicants should review their proposals for completeness, ensuring they meet the required format and page/word limits specified in the Open Call guidelines. The platform provides validation to ensure all mandatory fields are filled.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Step 4 - Submission Confirmation**: Once the proposal is submitted, applicants will receive a confirmation email from the F6S platform with a unique reference number for their application. This number should be retained for future reference.

5.2.2 Review Process

The review process for the CyberSecDome Open Call is designed to be fair, transparent, and rigorous, ensuring that only high-quality proposals are funded. The process is divided into several stages:

Stage 1: Eligibility Check

The first step is an eligibility check to ensure that proposals meet the minimum eligibility criteria. This includes checking:

- **Applicant eligibility**: Applicants must be from eligible countries and meet the Open Call's conditions (as described in **Annex 5.1.4 and 5.8**).
- **Proposal completeness**: Proposals must be complete, with all sections completed, and comply with the specified format.
- **Proposal limits**: Proposals must adhere to the page and word limits for each section. Proposals exceeding these limits will be automatically disqualified.

Only proposals that pass the eligibility check will proceed to the next stage.

Stage 2: Evaluation by Expert Panel

An independent panel of external evaluator experts from academia and industry with expertise in cybersecurity, AI, and VR technologies will evaluate eligible proposals.
The evaluation will be based on the following criteria:

- **Excellence**: The quality and innovation of the proposal in addressing the cybersecurity challenges outlined in the Open Call.
- **Impact**: The potential business and technical impact of the proposal, as well as the sustainability of the solution after the project's completion.
- **Implementation**: The feasibility and quality of the work plan, including the budget allocation, resource distribution, and risk management strategies.

Each criterion will be scored on a scale of **0 to 5**, and only proposals that meet the minimum threshold for each criterion will be considered for funding. The final score will be a weighted combination of the three evaluation criteria. Stage 2 will progressively take place as follows:

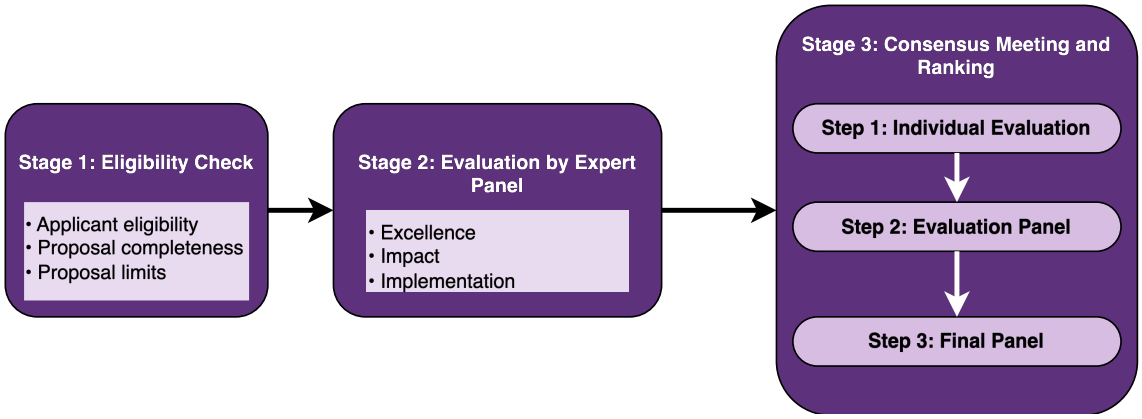
- ***Step 1—Individual Evaluation***: Each proposal will be assigned to at least **three Cybersecdome expert evaluators**. Each evaluator will provide a signed individual evaluation form and assess the proposal that has passed the initial eligibility verification check in the above-mentioned categories of criteria.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- ***Step 2—Evaluation panel***: Following individual evaluation, the experts will have a consensus remote meeting to agree on a **consensus-signed evaluation form** summarising common evaluation text and the proposal score. The proposals over the threshold may be invited for an online interview to clarify questions and explain their proposal.
- ***Step 3—Final Panel:*** To smooth any human factors, all evaluators will have a joint panel remote (online) meeting to rank and shortlist the proposals. The questions to be assessed by the jury of experts and the procedure to untie proposals are defined in the Round Specific document.

Stage 3: Consensus Meeting and Ranking

Once the expert panel has completed the evaluations, **a consensus meeting between the Evaluators Group and the Open Call Management Team (OCMT)** will be held to discuss the proposals and finalise the scores. Proposals that meet the minimum threshold for each criterion will be ranked according to their overall score, and a final list of eligible successfully ranked funding proposals will be created.



The OCMT ultimately decides on funding proposals. If they find that there aren't enough high-quality proposals, they may either forgo making selections or choose fewer than allowed by the Call. Furthermore, the OCMT will review the selected proposals from a portfolio perspective, ensuring a diverse range of use cases to better evaluate the Cybersecdome's potential capabilities. This review is required when proposals do not meet the threshold outlined in the attached evaluation form. Should the number of selections prove inadequate, the Consortium has the right to reopen the Call in the future.

5.2.3 Feedback and Next Steps

After completing the evaluation process, all applicants will receive detailed feedback on their proposals. This feedback will include:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Strengths and Weaknesses**: A summary of the evaluation panel's assessment, highlighting the strengths and weaknesses of the proposal. This section will provide insight into the areas where the proposal excelled and areas for improvement.
- **Final Score**: The proposal's overall score, along with a breakdown of the scores for each evaluation criterion (Alignment, Excellence, Impact, Implementation, and Value for Money).
- **Go/No-Go Decision**: A final decision on whether the proposal has been selected for funding based on the evaluation scores and the panel's overall assessment.

According to the timeline specified in the Open Call Round 1 General Guide, applicants will receive this feedback approximately five weeks after the round deadline.

5.2.3.1 Go Outcomes and Change Requests

- Applicants with a Go outcome may also receive requests for changes or clarifications to their proposal. These could include adjustments to the project content, such as outputs, KPIs, descriptions, and/or budget changes.
- Applicants must implement the requested changes as indicated in the feedback provided through the submission system. Once the necessary adjustments are made, the revised proposal must be resubmitted for final approval.
- Go outcome proposals are expected to commence on the first day of the project execution timeframe as defined in the Open Call Round 1 General Guide. All efforts and expenses reported outside this timeframe will not be considered eligible for funding.

5.2.3.2 No-Go Outcomes and Further Steps

Applicants whose proposals receive a **No-Go** outcome will be encouraged to review the feedback carefully and consider resubmitting an improved proposal for **Round 2**, if applicable. These applicants are welcome to contact the CyberSecDome support team to discuss the feedback and seek guidance on improving their proposals for future rounds.

5.2.3.3 Consortium Rights

- The CyberSecDome consortium, at its sole discretion, reserves the right to make exceptions to the feedback and evaluation process on a case-by-case basis, should the OCMT deem it necessary.
- Additionally, the CyberSecDome consortium retains the right to allocate all, part, or none of the available budget for Round 1, depending on the quality of the proposals submitted. If there are insufficient high-quality proposals, the consortium may choose not to allocate the entire budget for this round.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5.2.4 Appeal Procedure

The CyberSecDome consortium will, in good faith, address any potential disputes related to the evaluation and selection process outlined in this document. If an applicant believes there has been a procedural error or oversight during the evaluation process, they may submit an appeal. Appeals must be based on factual evidence of the error and not merely a disagreement with the outcome or scores assigned.

5.2.4.1 Process for Submitting an Appeal

- **Timing**: Appeals must be submitted within **five (5) working days** of receiving the evaluation results. This includes either the rejection letter (in case of non-eligibility) or the Evaluation Summary Report (ESR).
- **Grounds for Appeal**: Appeals should clearly outline the procedural error or discrepancy during the evaluation. Appeals will only be accepted if there is evidence that a procedural error during the review process has affected the outcome. Disagreements solely based on the evaluation scores or final decision will not be considered.

5.2.4.2 Internal Review and Re-Evaluation

- Upon receiving an appeal, the OCMT will review the request and determine whether a re-evaluation is warranted.
- An internal review committee will be established to examine the case. The committee will assess the facts presented, including the procedural aspects of the evaluation process.
- If there is clear evidence that a procedural error occurred, and this error could potentially affect the funding decision, the proposal or parts of it may be re-evaluated.
- Any change requests or outcomes resulting from the appeal will be communicated to the applicant following the review process.

Note: The CyberSecDome consortium reserves the right to make exceptions to the appeal procedure on a case-by-case basis should the OCMT deem it necessary.

5.2.5 Risk Considerations

Considering the CyberSecDome consortium's responsibility to distribute public funding without taking unnecessary risks, the OCMT reserves the right not to support proposals, regardless of their scoring, if the risk profile is deemed too high. This includes, but is not limited to, financial, technical, operational, and reputational risks.
The evaluation panel will assess the risk level associated with each proposal during the review process. This evaluation will consider:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Financial Risk**: Proposals with weak financial capacity or those that cannot demonstrate the ability to co-fund, if necessary, may be excluded from funding, even if their technical evaluation is strong.
- **Operational Risk**: Proposals that present significant challenges in terms of implementation, timelines, or resources may be deemed too risky. This could include over-ambitious project scopes or reliance on unproven technologies.
- **Reputational Risk**: Proposals involving entities or projects that could pose a reputational risk to the CyberSecDome consortium or the European Union will also be excluded. This includes concerns about unethical practices, prior controversies, or significant operational challenges in past projects.

Additionally, CyberSecDome Consortium may choose to withhold or limit funding if:

- **Due Diligence Outcomes**: As part of the due diligence process, the OCMT identifies issues with the applicant's financial stability, legal status, or capacity to fulfil the project's obligations.
- **Compliance with EU Rules**: If the applicant or any project partner is found to be non-compliant with EU regulations or involved in activities that conflict with the Horizon Europe guidelines.

CyberSecDome consortium retains the right to make discretionary decisions regarding the allocation of funds, including the possibility of rejecting high-scoring proposals if the overall risk is deemed too great.

5.3 Annex C: Evaluation Criteria

The **CyberSecDome Open Call** follows a rigorous evaluation process to ensure that the most innovative, impactful, and feasible proposals are selected for funding. The evaluation criteria are aligned with the **Horizon Europe** framework and focus five key criteria: **Alignment**, **Excellence**, **Impact**, **Implementation**, and **Value for Money**. Each criterion will be scored between 0 and 5, and proposals must meet a minimum threshold score in each criterion to be considered for funding.

Each proposal will be evaluated by an independent panel of experts, who will assign scores based on the following criteria:

5.3.1 Alignment

This criterion assesses how well the proposal aligns with the objectives and challenges outlined in the CyberSecDome Open Call. Proposals must clearly show that they are directly addressing the core use cases and technical goals of the project.

Key elements evaluated under Alignment include:

- **Relevance to Open Call objectives**: Proposals should clearly demonstrate how they address the specific cybersecurity challenges outlined in the Open Call

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

topics. The use cases proposed should be well-defined and focus on solving problems within the CyberSecDome framework.

- **Key Performance Indicators (KPIs):** The proposal should include relevant KPIs that measure the effectiveness of the solution. These KPIs should align with the project's broader goals and be used to monitor progress throughout the project lifecycle.
- **Fit within CyberSecDome**: Proposals must demonstrate that the use case or technology fits well within the existing CyberSecDome environment and technical architecture.

Scoring: The Alignment criterion will be scored on a scale of 0 to 5, with a minimum threshold score of 3 required for the proposal to proceed.

5.3.2 Excellence

This criterion evaluates the scientific and technical quality, ambition, and innovation of the proposed project. Proposals should clearly define the problem, the objectives, and the innovative approach used to solve the cybersecurity challenges.

Key elements evaluated under Excellence include:

- **Clarity and relevance of objectives**: Proposals should have clear, specific, and measurable objectives that align with the challenges outlined in the Open Call. These objectives should demonstrate a deep understanding of the problem being addressed.
- **Innovative approach**: Proposals must present a novel solution to the identified cybersecurity challenges. This could involve applying new methods, technologies (such as AI or VR), or using existing tools in innovative ways.
- **Technical soundness**: Proposals should provide detailed information about the technical methods and tools being used, showing that the approach is scientifically and technically feasible. The methodologies should be well thought out and applicable to real-world scenarios.
- **Alignment with CyberSecDome objectives**: Proposals must clearly show how they align with the overall goals of CyberSecDome, particularly in enhancing cybersecurity resilience through the use of AI and VR technologies.

Scoring: The Excellence criterion will be scored on a scale of 0 to 5, with a minimum threshold score of 3.

5.3.3 Impact

The Impact criterion assesses the potential of the project to generate significant, measurable benefits for the cybersecurity community, industry stakeholders, and the broader digital ecosystem in Europe.

Key elements evaluated under Impact include:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Technical and business impact:** Proposals should define the expected improvements in cybersecurity resilience, such as reduced incident detection and response times, enhanced protection mechanisms, or improved scalability of solutions. These improvements should benefit both the technical and business aspects of cybersecurity.
- **Exploitation and dissemination plans:** Applicants must provide clear plans for how they intend to exploit the project's results both during and after the funding period. This could include commercial applications, partnerships, or scaling the solution across different industries. Additionally, the dissemination plan should detail how the project outcomes will be communicated to relevant stakeholders and the public.
- **Sustainability:** Proposals must include a strategy for sustaining the solution beyond the funding period. This could involve business models, ongoing partnerships, or securing additional funding to continue the project.
- **KPIs:** Proposals should include clear, measurable KPIs that will be used to track the project's success. These indicators should cover both technical outcomes (such as threat detection accuracy or incident response times) and business impact (such as cost savings or scalability).

Scoring: The Impact criterion will be scored on a scale of 0 to 5, with a minimum threshold score of 3 required for the proposal to remain eligible for funding.

5.3.4 Implementation

This criterion evaluates the feasibility and quality of the proposed work plan, the allocation of resources, and the project's risk management strategies. The proposal should provide a clear roadmap for delivering the project objectives, with a breakdown of tasks, timelines, and deliverables.

Key elements evaluated under Implementation include:

- **Work Plan**: Proposals must present a detailed work plan that outlines all tasks, timelines, milestones, and deliverables. The plan should show how the project will be completed within the proposed timeframe, including the design, implementation, and demonstration phases. The plan should be realistic and demonstrate a solid understanding of the necessary steps to achieve the project goals.
- **Resource Allocation**: Proposals should clearly explain how resources (personnel, equipment, subcontracting, etc.) will be allocated to each task. The budget should be aligned with the work plan and justified concerning the proposed outcomes. Applicants must demonstrate that the resources allocated are adequate and appropriate for the tasks outlined.
- **Risk Management**: A thorough risk management strategy must be included. This should identify potential risks (technical, operational, or financial) and propose

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

mitigation measures to address those risks. The strategy should be proactive and reflect an understanding of the possible challenges.

- **Team Expertise**: The qualifications and experience of the project team will also be evaluated. Proposals must show that the team has the necessary skills, experience, and capabilities to implement the project successfully. This includes past experience in similar projects, technical expertise, and the composition of the team (e.g., multidisciplinary or gender-balanced teams).

Scoring: The Implementation criterion will be scored on a scale of **0 to 5**, with a minimum threshold score of **3** required for the proposal to be considered for funding.

5.3.5 Value for Money

The Value for Money criterion evaluates the efficiency and cost-effectiveness of the proposed project. The proposal should demonstrate that the project will deliver high value concerning the amount of funding requested and the resources deployed.
Key elements evaluated under Value for Money include:

- **Budget justification:** Proposals must present a clear, detailed budget that aligns with the work plan and shows how the funding will be used effectively to achieve the project's objectives. The budget should demonstrate that the project is using resources efficiently and that there is no unnecessary expenditure.
- **Cost-effectiveness**: Proposals should demonstrate how the funding will lead to meaningful and impactful results. The project must provide a strong return on investment in terms of both technical advancements and business benefits.
- **Leveraging additional resources**: Where possible, proposals should show how they intend to leverage additional resources (e.g., through partnerships, collaborations, or other funding sources) to maximize the impact of the project.
- **Overall resource management**: The proposal should include a comprehensive plan for managing the project's resources, ensuring that personnel, equipment, and other assets are used efficiently and contribute to the success of the project.

Scoring: The Value for Money criterion will be scored on a scale of 0 to 5, with a minimum threshold score of 3 required.

5.3.6 Overall Scoring and Thresholds

Each criterion (Alignment, Excellence, Impact, Implementation, and Value for Money) will be scored individually on a scale of **0 to 5**, with a minimum threshold score of **3** for each criterion:

Score	Description
0	Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

1	Poor – The criterion is inadequately addressed, with serious weaknesses.
2	Fair – The proposal broadly addresses the criterion but with significant weaknesses.
3	Good – The proposal addresses the criterion well, but improvements are needed.
4	Very Good – The proposal addresses the criterion very well, with only minor improvements needed.
5	Excellent – The proposal successfully addresses all aspects of the criterion in a highly comprehensive and effective manner.

5.3.6.1 Minimum Thresholds and Weighting:

To be eligible for funding, **a proposal must meet the minimum threshold score of 3** in each of the five evaluation criteria. Proposals that fail to meet the threshold in any criterion will not proceed to the following evaluation stage.

The overall score will be a weighted combination of the following criteria:

- ***Alignment***: 20% of the final score
- ***Excellence:*** 30% of the final score
- ***Impact:*** 30% of the final score
- ***Implementation:*** 10% of the final score
- ***Value for Money***: 10% of the final score

Example of Scoring Breakdown:

- Alignment: If the proposal scores 4/5 in Alignment, the weighted contribution would be (4/5) * 20% = 16% of the final score.
- Excellence: If the proposal scores 3/5 in Excellence, the weighted contribution would be (3/5) * 30% = 18% of the final score.

In the Event of a Tie: If two or more proposals receive the same final score, the Impact score will be the deciding factor.

5.4 Annex D: Costs Reporting and Key Performance Indicators (KPIs)

This annex provides essential guidance on the **financial reporting requirements** and the **Key Performance Indicators (KPIs)** that projects will be evaluated against during and after implementation. Applicants must adhere to these guidelines for proper financial management and successfully delivering the project's objectives.

5.4.1 Cost Reporting

The cost reporting guidelines for the CyberSecDome Open Call are based on the principles set out in the **Horizon Europe Model Grant Agreement (MGA)** and also in the

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

CyberSecDome Third-Party Funding Agreement (TPFA). All eligible costs must be reported accurately and in compliance with EU funding rules.

5.4.1.1 Eligible Costs

The following costs are considered eligible under the CyberSecDome Open Call:

- **Personnel Costs**: Salaries, social security contributions, and other costs linked to the employment of staff directly involved in the project.
- **Subcontracting Costs**: Costs for work or services required to complete project tasks, outsourced to third-party providers.
- **Purchase Costs**: Including equipment, materials, software, and licenses directly required for the project's execution.
- **Other Direct Costs**: Travel costs, accommodation, and other directly attributable costs necessary for project completion.
- **Indirect Costs**: Calculated as a flat rate of **25% of eligible direct costs**(excluding subcontracting costs and other specified categories). Indirect costs cover overhead expenses such as utilities, rent, and administrative support.

5.4.1.2 Ineligible Costs

Certain costs are not eligible for funding under the CyberSecDome Open Call, including but not limited to:

- Costs incurred before the official start date of the project.
- Costs unrelated to project activities, including general administrative overheads that are not directly linked to the project execution.
- Costs associated with debt servicing, interest payments, or losses from currency exchange rate fluctuations.
- Costs for contributions in kind, such as volunteer work or non-paid efforts.

5.4.1.3 Key Reporting Considerations

All budget information must be precise and aligned with the rules set out in the HORIZON EUROPE Model Grant Agreement (MGA) and CyberSecDome Third-Party Funding Agreement (TPFA). The proposal must assign the budget to the correct cost categories as outlined in the Horizon Europe guidelines.

- **Action Definition**: In cost reporting, the term **"action"** refers to the activities within the CyberSecDome project. All costs must be allocated to one or more specific project tasks.
- **Task-Based Costing**: Costs must be attributed to the respective tasks within the project. Task budgeting can be based on planning assumptions, while the actual reporting must reflect actual costs incurred. Reported costs should not exceed the approved budget for each task.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Subcontracting**: Subcontracting must be explicitly defined in the proposal and should comply with value-for-money principles and conflict-of-interest regulations. Subcontracting costs must also follow all applicable rules outlined in the CFSA.
- **Full-Time Equivalents (FTEs)**: It is strongly recommended that each Task Leader/Contributor commits at least **0.2 FTEs** to ensure meaningful involvement and adequate resource allocation for the task.

5.4.1.4 Reporting Deadlines

To ensure proper financial management, projects must adhere to the following deadlines for cost reporting:

- **Initial Report**: Submitted within **six (6) months** of the project start date, outlining the initial expenditure and budgetary adjustments if necessary.
- **Interim Report**: A comprehensive financial report is required at the project's mid-point, typically **M9**, detailing all costs incurred to date, including personnel, subcontracting, and other direct costs.
- **Final Report**: Upon project completion, a complete financial report must be submitted no later than **30 days** after the project end date. This report must provide a detailed breakdown of all eligible costs and supporting documentation.

5.4.2 Grant Payments

Grant payments will be made based on the submission of accurate and timely cost reports. The following payment schedule applies:

- **Initial Payment (30%)**: Paid upon signing the **CyberSecDome Third-Party Funding Agreement (TPFA)** by all parties (M1).
- **Interim Payment (Up to 30%)**: Based on the outcome of the **Interim Assessment** at M9. This payment will be contingent on the satisfactory completion of the project's initial milestones and the submission of the interim report.
- **Final Payment**: The remaining balance will be paid upon successfully completing the project and obtaining approval for the final report.

Failure to submit accurate cost reports or meet key milestones may result in delays or reductions in grant payments.

5.4.3 Key Performance Indicators (KPIs)

KPIs play a crucial role in measuring the success of the project. They are designed to evaluate both the **technical performance** and the **business impact** of the proposed solution. Applicants must define and track KPIs throughout the project's lifecycle. These must follow the classical SMART criteria:

- ***Specific:*** clearly defined and concrete
- ***Measurables:*** easy to measure based on quantitative data

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- ***Achievable:*** Demanding but achievable in the project framework
- ***Relevant:*** Aligned with the CyberSecDome objectives
- ***Time-based:*** to be achieved during the project timeframe

There are two types of KPIs:

- **CyberSecDome defined KPIs**: The CyberSecDome team defines some specific objectives for each round that all proposals must share.
- **Proposal-defined KPIs**: Aligned with each proposal's objectives, the applicants must describe specific KPIs to be achieved in the project.

Those KPIs will be one of the main criteria to evaluate the performance of the project.

Please note that the CyberSecDome consortium may apply financial penalties in case of clear underdelivery, including underachievements in any of the categories of targets and KPIs described above.

5.4.3.1 Technical KPIs

Technical KPIs will assess the effectiveness of the cybersecurity solution in real-world or simulated environments. Examples of technical KPIs include:

- **Threat detection rate**: The percentage of detected cybersecurity threats relative to the total number of simulated or real-world threats.
- **Incident response time**: The time taken to detect, assess, and respond to a cybersecurity incident.
- **System resilience**: The ability of the system to maintain operational integrity in the face of cybersecurity attacks or system failures.
- **False positive/false negative rate**: The system's accuracy in distinguishing legitimate threats from false alarms.

5.4.3.2 Business KPIs

Business KPIs will measure the broader impact of the project on organisational goals and the cybersecurity market. Examples of business KPIs include:

- **Cost savings**: The reduction in operational costs related to cybersecurity incident management and prevention.
- **Market scalability**: The ability of the solution to be scaled across different industries or sectors.
- **User adoption rate**: The number of users or organisations that adopt the solution after the project's completion.
- **Commercial viability**: The potential for the solution to generate revenue or secure additional investment post-project.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5.4.3.3 Reporting on KPIs

Projects must report their KPIs as part of the **Interim Report** and **Final Report**. These reports must include:

- A detailed description of how the KPIs were measured.
- Data supporting the achievement of each KPI, including any quantitative or qualitative evidence.
- An explanation of any deviations from the expected KPI targets, along with reasons and mitigation strategies, if necessary.

5.4.4 Compliance and Auditing

All cost reports and KPI submissions are subject to review and audit by the **CyberSecDome Open Call Management Team (OCMT)** and the **CyberSecDome Open Call Implementation Team (OCIT).** Applicants must ensure that all expenses and performance metrics are accurately reported, and they must maintain all supporting documentation for auditing purposes.

Key compliance points include:

- **Documentation**: Applicants must keep detailed records of all project costs, including invoices, receipts, and contracts. These documents must be retained for up to **five years** after the project's completion.
- **KPI Verification**: KPIs must be based on verifiable data, and supporting evidence must be provided in reports.
- **Audit Rights**: The CyberSecDome consortium reserves the right to audit projects during and after the funding period to ensure compliance with the terms of the CyberSecDome Third-Party Funding Agreement (TPFA).

5.5 Annex E: Communication, Dissemination, and Visibility

Successful applicants must ensure effective communication and dissemination of their project results and activities in line with **Horizon Europe's guidelines** and the **CyberSecDome project's objectives**. This annex outlines the requirements for communication, dissemination, and visibility, ensuring that the outcomes of the CyberSecDome Open Call are made widely available to the appropriate stakeholders and the general public.

5.5.1 Communication Plan

Each funded project must develop and implement a comprehensive **Communication Plan**. The purpose of the plan is to ensure that the project's results are clearly communicated to stakeholders, end-users, and the wider public in a timely and effective manner.

The Communication Plan should include:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Target Audience**: Define the key stakeholders who will benefit from or be interested in the project's results. This may include public sector entities, private companies, research institutions, cybersecurity professionals, and policy-makers.
- **Communication Channels**: Identify the channels that will be used to disseminate project updates and results. This may include:
    - **Project website** or a dedicated page on the applicant's website.
    - **Social media platforms** (e.g., LinkedIn, Twitter, YouTube) to share progress, news, and results.
    - **Press releases** and **media articles** in industry or academic publications.
    - **Newsletters** sent to subscribers and stakeholders.
- **Key Messages**: Clearly outline the project's objectives, the challenges it addresses, and its expected impact on cybersecurity. Ensure that all communication materials are aligned with the CyberSecDome project's overarching message of improving cybersecurity through AI and VR.
- **Timeline**: Provide a timeline for the dissemination activities, including major milestones such as the project's launch, interim results, and final outcomes.

All communication materials must acknowledge the financial support received from **Horizon Europe**.

5.5.2 Dissemination of Results

Dissemination activities are crucial for ensuring that the results of the CyberSecDome Open Call projects reach the appropriate audiences and contribute to the wider adoption of cybersecurity solutions. The goal is to make the project's findings and tools accessible to other researchers, policymakers, and industry practitioners.

Key dissemination activities include:

- **Publication of Results**: Project results should be published in relevant academic or industry journals, conference proceedings, and other platforms to ensure visibility in the cybersecurity research community.
- **Open Access**: In compliance with Horizon Europe's Open Access policy, publications resulting from the project must be made available through open-access platforms or repositories, where applicable.
- **Workshops and Webinars**: Organize or participate in workshops, webinars, or conferences to share project findings and promote discussions with stakeholders. This may include presentations at industry events, research symposia, or EU-organized cybersecurity forums.
- **Collaboration with Other Projects**: Where relevant, project teams should collaborate with other EU-funded cybersecurity initiatives to ensure cross-project learning and avoid duplication of efforts.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5.5.3 Visibility Guidelines

Unless otherwise agreed with the CyberSecDome consortium, all communication and dissemination activities and materials (including media relations, conferences, seminars, and information material, such as brochures, leaflets, posters, presentations, papers etc., in electronic form, via traditional or social media, etc) produced by those participating in the Open Call as well as any infrastructure, equipment, vehicles, supplies or major outcome of the participating projects must comply with the **Horizon Europe visibility guidelines**.[5] This includes displaying the **EU emblem** and acknowledging the funding received under the CyberSecDome project with **a funding statement** (translated into local languages where appropriate). The following elements must be included in all public-facing materials:

- **EU Emblem & Acknoledgement of Funding**: The EU emblem must be prominently displayed on all communication materials, including the project website, publications, presentations, and brochures. In all public communications (including social media posts, articles, and presentations), the applicant must acknowledge the support of the European Union and the CyberSecDome project. Therefore the emblem should be accompanied by the text: "***This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101120779.***" The emblem must remain distinct and separate and cannot be modified by adding other visual marks, brands or text. Apart from the emblem, no other visual identity or logo may be used to highlight the EU support. When displayed in association with other logos (e.g. logos of partners), the emblem must be displayed at least as prominently and visibly as the other logos. For the purposes of their obligations under this Article, the partners may use the emblem without first obtaining approval from CyberSecDome consortium. This does not, however, give them the right to exclusive use. Moreover, they may not appropriate the emblem or any similar trademark or logo, either by registration or by any other means.
- **CyberSecDome Branding**: The CyberSecDome project logo and branding must be used consistently across all materials to ensure alignment with the project's visual identity. This includes following CyberSecDome's guidelines on using fonts, colors, and logos in communications.
- **Quality of Information**: Any communication or dissemination activity related to the Innovation Activity must use factually accurate information. Moreover, it must indicate the following disclaimer (translated into local languages where appropriate): ***"Funded by the European Union. Views and opinions expressed***

[5] https://commission.europa.eu/funding-tenders/managing-your-project/communicating-and-raising-eu-visibility_en

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

are, however those of the author(s) only and do not necessarily reflect those of the European Union or CyberSecDome. Neither the European Union nor the granting authority can be held responsible for them."

Co-funded by the European Union

5.5.4 Reporting on Communication and Dissemination Activities

Projects are required to report on their communication and dissemination efforts regularly. These reports should include:

- **Activity Summary**: A brief overview of the communication and dissemination activities carried out during the reporting period (e.g., events organised, publications produced, articles published).
- **Key Metrics**: Data on the reach and engagement of the dissemination activities, including website traffic, social media metrics (e.g., followers, impressions, engagement), and the number of participants in workshops or webinars.
- **Challenges and Adjustments**: An overview of any challenges encountered during the implementation of the Communication Plan, along with adjustments made to improve the effectiveness of outreach efforts.

These reports should be included in the **Interim Report** and **Final Report** to the CyberSecDome consortium. Failure to comply with the communication and dissemination requirements may delay grant payments.

5.5.5 Events and Publicity

Unless otherwise agreed with CyberSecDome consortium, the organizations of the selected proposals must promote the activity and its results by providing targeted information to multiple audiences (including the media and the public). That said, before engaging in a communication or dissemination activity expected to have a major media impact, the partners must inform CyberSecDome consortium. To maximise the visibility of project results, project teams are encouraged to:

- **Participate in EU-organized events**: Engage with events organized by the European Commission or Horizon Europe, such as cybersecurity conferences, information days, or thematic workshops.
- **Organize Project-Specific Events**: Host events such as launch events, demonstrations, or project showcases to promote the project's milestones and achievements to a wider audience.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Collaborate with the CyberSecDome Consortium**: Collaborate closely with the CyberSecDome communications team to ensure alignment with the broader project's messaging and communication goals. This includes sharing major achievements or milestones with the consortium for inclusion in project-wide dissemination efforts.

5.6 Annex F: Intellectual Property Rights (IPR)

The management of **Intellectual Property Rights (IPR)** is crucial to the success of the CyberSecDome Open Call projects, ensuring that project results are protected and can be exploited in alignment with both the consortium's and the participants' goals. This annex outlines the key principles governing IPR and the responsibilities of applicants regarding the ownership, protection, and exploitation of intellectual property created during the project.

5.6.1 IPR Framework

The CyberSecDome Open Call follows the Intellectual Property Rights rules (Article 16) under the **HORIZON EUROPE MGA** for Intellectual Property Rights. Applicants must ensure compliance with these rules to protect their project results while facilitating collaboration with other participants.

The key objectives of the IPR framework are to

- Ensure **ownership and protection** of intellectual property generated during the project.
- Facilitate **access and usage rights** to IP among project partners, where necessary.
- Promote the **exploitation** of project results in line with the goals of CyberSecDome and the European Union.

5.6.2 Ownership of Results

Ownership of intellectual property created during the project will remain with the participant(s) that generate it. Each project partner retains ownership of the intellectual property they develop, but they are required to comply with the relevant **IPR provisions** to ensure the fair use of shared resources and results.

Key principles include:

- **Sole Ownership**: The entity (whether an SME, research institution, or industry partner) that develops the intellectual property owns the results unless otherwise agreed by the consortium.
- **Joint Ownership**: In cases where intellectual property is jointly developed by multiple partners, joint ownership rules will apply. Joint owners must negotiate and agree on the division of ownership and the terms of exploitation. This agreement must comply with Horizon Europe guidelines.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

All participants must ensure that any background IP (existing intellectual property) brought into the project and required for the implementation of the project is clearly identified and agreed upon at the start of the project.

5.6.3 Protection of Results

Participants must ensure the appropriate protection of their intellectual property to enable future commercial exploitation. This may include patenting, copyrighting, or other formal protection mechanisms, depending on the nature of the IP.
Steps to protect intellectual property include:

- **Filing Patents**: Where applicable, participants are encouraged to file patents to protect any innovative solutions, inventions, or technologies developed during the project.
- **Trademarking and Copyrighting**: Participants should explore trademarking or copyrighting any project outputs that may need protection to prevent unauthorised use or duplication by third parties.
- **Confidentiality Agreements**: To protect sensitive project information, partners should enter into confidentiality or non-disclosure agreements (NDAs) when sharing proprietary knowledge with third parties or consortium members.

Participants should also seek legal advice, if necessary, to ensure that their intellectual property is protected according to the best industry practices and aligned with the regulatory framework of the European Union.

5.6.4 Access Rights

Access rights are granted to allow project partners to use each other's background or foreground IP to successfully complete the project. This ensures that collaboration within the consortium is supported while respecting the ownership rights of each partner.
Background IP: Background IP refers to pre-existing intellectual property or know-how that a participant brings into the project. Participants must agree on access rights to background IP before the project begins. Access to background IP should be granted on fair and reasonable terms if it is necessary for the execution of project tasks or the exploitation of results.
Foreground IP: Foreground IP refers to new intellectual property generated during the project. Access rights to foreground IP may be granted to other project partners under fair, reasonable, and non-discriminatory (FRAND) terms if required for the continuation of the project or further exploitation.

The following access rights rules apply:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Access for Project Implementation**: All partners will have access to the necessary background and foreground IP for the sole purpose of completing project tasks. This access is typically royalty-free.
- **Access for Exploitation**: Partners may negotiate access to IP for further exploitation, such as commercialization, after the project ends. The terms of this access will be determined by the consortium agreement and may include royalty payments or other financial terms.
- **Third-Party Access**: Any access rights granted to third parties (outside the project consortium) must be agreed upon by the IP owner and must not infringe on the project's terms or any other partner's rights.

5.6.5 Exploitation of Results

The results generated during the project must be exploited in alignment with the goals of CyberSecDome and Horizon Europe, focusing on maximising the value and impact of the results within the European cybersecurity sector.
Exploitation activities may include:

- **Commercialisation**: The commercialisation of new technologies, tools, or products developed during the project. Partners should outline their commercialisation strategies in the proposal phase, including potential markets, revenue streams, and business models.
- **Licensing**: Project partners may license their IP to other companies or organisations to enable further development and market adoption. Licensing agreements must comply with EU competition rules and Horizon Europe regulations.
- **Further Research**: Intellectual property can be used in future research and development projects. Participants should outline how they intend to use the IP for further innovation or collaboration in future projects.
- **Public Interest**: In certain cases, results may be made available for free or on open-access platforms if doing so serves the broader public interest (e.g., improving public sector cybersecurity solutions).

All participants must submit an **exploitation plan** outlining how they will use the project results after completing the project. This plan will be part of the **Final Report** and will be evaluated as part of the project's impact assessment.

5.6.6 IPR Reporting and Compliance

Participants are required to report on IPR management and protection measures as part of the project's regular reporting schedule. This includes:

- **IP Declarations**: All new IP generated during the project must be reported to the CyberSecDome consortium.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **IPR Section in Reports**: A section on IPR management and exploitation must be included in both the **Interim Report** and the **Final Report**. This section should detail the IP generated, how it has been protected, and the planned exploitation activities.
- **Compliance Audits**: The CyberSecDome consortium and Horizon Europe authorities reserve the right to audit the IPR activities of participants to ensure compliance with the CyberSecDome Third-Party Funding Agreement (TPFA) and EU regulations.

5.7 Annex G: Data Management Plan (DMP)

A **Data Management Plan (DMP)** is essential for ensuring that all data generated or collected during the CyberSecDome project is handled in a secure, transparent, and compliant manner. This annex outlines the requirements for data management, including collection, storage, protection, and sharing of data, in line with the principles of Horizon Europe and the General Data Protection Regulation (GDPR).

All applicants must submit a comprehensive DMP as part of their proposal, which will be updated and maintained throughout the project lifecycle. The plan will need to describe the data management life cycle for the data to be collected, processed, and/or generated by a project in accordance with FAIR (Findable, Accessible, Interoperable, Reusable) principles. More information can be found in the **HORIZON EUROPE MGA**.

5.7.1 Overview of the Data Management Plan

The DMP should provide a detailed strategy for how data will be handled during and after the project, ensuring that:

- **Data is managed responsibly** and in compliance with applicable laws and standards.
- **Data quality** is maintained throughout the project.
- **Data protection measures** are in place to safeguard sensitive information.
- **Data sharing** is facilitated where necessary to ensure transparency and support future research.

The DMP should cover the following aspects in detail:

5.7.2 Data Collection

Applicants must describe what types of data will be collected, processed, or generated during the project. This section should address:

- **Types of Data**: The categories of data that will be collected or generated, such as personal data, cybersecurity logs, network traffic data, user behavioral data, and system performance metrics.
- **Data Formats**: The specific formats in which the data will be collected and stored (e.g., CSV, JSON, XML, PCAP files, log files, etc.).

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Metadata**: Details of the metadata that will describe the data, including documentation standards, so that the data can be understood and reused by others.
- **Data Collection Methods**: The tools, software, or systems used to collect the data (e.g., network monitoring tools, threat detection systems, penetration testing logs).

5.7.3 Data Storage

Applicants must describe how the collected data will be stored securely throughout the project, including:

- **Storage Location**: Specify the storage infrastructure that will be used (e.g., cloud storage, on-premise servers, external data centers). Ensure that the storage solution is robust and scalable
- **Data Access**: Define who will have access to the stored data, including team members, partners, and stakeholders. Access rights should be clearly specified, and administrative controls should be in place to prevent unauthorized access.
- **Backup and Recovery**: Include procedures for regular data backup and recovery to prevent data loss due to system failure, corruption, or cyberattacks.
- **Data Retention Periods**: Specify how long the data will be stored and when it will be deleted or archived after the project is completed.

5.7.4 Data Protection

Data protection is a key element of the DMP, particularly when handling personal data or sensitive information. Applicants must ensure that their data protection plan complies with the **GDPR** and other relevant data protection laws.

The DMP should address the following data protection issues:

- **Personal Data**: If personal data is being collected (e.g., user or customer data), applicants must describe how they will ensure that the data is collected and processed lawfully, fairly, and transparently.
- **Consent and Anonymization**: Where personal data is involved, applicants must detail how they will obtain informed consent from individuals and how personal data will be anonymised or pseudonymised to protect privacy.
- **Data Security**: Describe the technical and organisational measures that will be implemented to safeguard the data from unauthorised access, theft, or tampering. This may include encryption, firewalls, intrusion detection systems, and secure access controls.
- **Data Breach Response**: Outline a response plan in case of a data breach, including how affected parties will be notified and how the breach will be mitigated.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

5.7.5 Data Sharing and Access

Projects must include a plan for how data will be shared both during and after the project. This section should detail:

- **Data Sharing with Partners**: If data will be shared with project partners or external entities, applicants must specify who will receive access, the conditions under which access will be granted, and any legal agreements (e.g., Data Sharing Agreements).
- **Open Data and Access to Results**: In line with **Horizon Europe's Open Access requirements,** applicants should describe how the project results and data will be made available to the public or research community, where applicable. Open access may be required for publications, datasets, or project findings to maximise the project's impact.
- **Data Repositories**: Specify which repositories or platforms will be used to share data (e.g., institutional repositories, open-access platforms like Zenodo). If there are any restrictions on data sharing (e.g., due to privacy concerns or proprietary data), these should be clearly stated.
- **Licensing and Usage Rights**: Define the terms of use for shared data, including licensing terms (e.g., Creative Commons) and restrictions on commercial use or redistribution.

5.7.6 Ethical Considerations

All projects must comply with ethical guidelines for data collection and management, particularly when handling sensitive data or engaging in activities that involve human subjects.

- **Ethics Approvals**: If the project involves collecting sensitive data or working with human subjects, applicants must seek the necessary ethics approvals from institutional review boards or ethics committees.
- **Informed Consent**: Ensure that informed consent is obtained from all individuals whose data is being collected or used. Participants must be fully aware of how their data will be used, stored, and shared.
- **Data Subject Rights**: Projects must ensure compliance with the rights of data subjects under the GDPR, including the right to access, rectify, or erase their personal data.

5.7.7 Monitoring and Reporting on Data Management

Projects are required to monitor their data management practices throughout the project lifecycle. A detailed DMP must be submitted as part of the **Interim Report** and **Final Report**, addressing the following:

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **DMP Updates**: Regular updates to the DMP should reflect any changes in the types of data being collected, new data protection measures, or changes in data sharing plans.
- **Data Quality Monitoring**: Projects must ensure that the data collected is of high quality, accurate, and complete. Data quality control procedures should be in place to prevent errors or inconsistencies in the data.
- **Audit and Compliance**: The CyberSecDome consortium may audit projects to ensure compliance with the DMP. Applicants must be prepared to provide documentation demonstrating adherence to the data management plan and GDPR.

5.8 Annex H: Applicant Conditions

The Applicant Conditions section outlines the key rules and requirements that all applicants must meet to be eligible for funding under the CyberSecDome Open Call. These conditions ensure fairness, transparency, and compliance with European Union regulations. Failure to meet these conditions may result in disqualification from the Open Call or the termination of funding agreements.

5.8.1 Eligibility Conditions

To participate in the CyberSecDome Open Call, applicants must comply with the following eligibility conditions:

- **Legal Entity Status**: Applicants must be legally established organisations within an EU Member State or a country associated with the Horizon Europe programme (as specified in Annex 5.1.4). This includes:
  - Micro, Small, and Medium-sized Enterprises (SMEs).
  - Large enterprises.
  - Research and academic institutions.
- **Financial and Ethical Requirements**: Applicants must:
  - Not have convictions for fraudulent behavior, financial irregularities, or unethical business practices.
  - Not have been declared bankrupt or initiated bankruptcy procedures.
  - Not be under liquidation or considered an enterprise in difficulty, as per Commission Regulation No 651/2014, Art. 2.18.
  - Not be excluded from the possibility of obtaining EU funding under both national and EU law or decisions by national or EU authorities.
- **Multiple Submissions**: Applicants can submit different proposals for different topics within Round 1 but must ensure they do not select multiple topics within a single proposal. If an applicant applies for Topic 1, no other topics may be selected by the same applicant in that round. This ensures focused, high-quality applications for each topic.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- **Resubmission for Round 2**: Applicants who applied for Round 1 and were not funded may resubmit a revised proposal for Round 2. However, applicants who received funding in Round 1 are ineligible to submit new proposals in Round 2 for the same activities.

5.8.2 Financial Capability

All applicants must demonstrate sufficient financial capability to support the costs associated with the project's execution. This includes the ability to finance the remaining costs not covered by the CyberSecDome grant (for instance, costs beyond the maximum grant limit of **€120,000**).

Applicants must meet the following financial requirements:

- **Proof of Financial Stability**: SMEs and large enterprises must show they have the necessary financial resources to maintain the project until the final grant payments are received. This may involve providing financial statements, balance sheets, or other financial documents during the evaluation phase to verify financial stability.
- **Full-Time Equivalent (FTE) Commitment**: It is recommended that each task leader/contributor commit at least 0.2 FTE to ensure meaningful involvement and adequate capacity for task execution.

Failure to demonstrate sufficient financial capability may result in the rejection of the proposal or delays in signing the CyberSecDome Third-Party Funding Agreement (TPFA).

5.8.3 Compliance with EU Regulations

All applicants must comply with European Union rules and regulations, ensuring that the project and its activities adhere to ethical, legal, and operational standards. Failure to comply with these regulations may lead to disqualification from the CyberSecDome Open Call or the withdrawal of funding.

Applicants must meet the following requirements:

- **Ethics and Integrity**:
  - Applicants must declare that they have not engaged in any illegal, fraudulent, or unethical activities. They must be free from any involvement in organised crime, corruption, money laundering, or terrorist financing.
  - Applicants must not have any criminal convictions for fraudulent or corrupt practices.
  - Applicants must not have any pending legal cases related to fraudulent activities or irregularities in the management of EU funding.
- **Bankruptcy or Liquidation**:
  - Applicants must not be under bankruptcy or liquidation proceedings, or any equivalent procedures in their country of establishment.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- Applicants must not be classified as an enterprise in difficulty, as defined by Commission Regulation No 651/2014, Art. 2.18, and must demonstrate that they are financially solvent and capable of fulfilling their project commitments.

- **Regulatory Compliance**:
  - Applicants must ensure that all activities conducted within the project comply with EU laws related to data protection (e.g., GDPR), intellectual property, cybersecurity, and any other relevant sector-specific regulations.
  - Compliance with EU environmental, health, and safety standards must also be guaranteed if applicable to the project's activities.

Applicants who fail to meet these compliance requirements will be deemed ineligible for funding under the CyberSecDome Open Call. If any non-compliance is discovered during project implementation, funding may be terminated.

5.8.4 Conflict of Interest

Applicants must declare any potential conflict of interest that may arise during the evaluation process or project implementation. A conflict of interest can undermine the fairness and impartiality of the proposal evaluation or project execution, and it must be disclosed to ensure transparency and ethical compliance.

5.8.4.1 Definition of Conflict of Interest

A conflict of interest may arise if:

- The applicant or any project team member has a personal, financial, or professional relationship with any member of the evaluation panel, CyberSecDome consortium, or any other entity involved in the Open Call.
- Any project team member has a vested interest or involvement that could compromise the impartiality or objectivity of the evaluation or project management process.

5.8.4.2 Notification Requirement

- Applicants are required to formally notify the CyberSecDome consortium without delay if any situation constituting or likely to lead to a conflict of interest is identified.
- Upon notification, the applicant must take immediate and appropriate measures to rectify the situation and avoid compromising the evaluation process or project implementation.

5.8.4.3 Consortium's Right to Review:

The CyberSecDome consortium and the granting authority may review the measures taken by the applicant to resolve the conflict of interest. If the consortium finds the

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

actions inadequate, they may require additional corrective steps to be taken within a specified deadline.

5.8.4.4 Consequences of Non-Compliance:

If an applicant fails to disclose a conflict of interest, or if the measures taken are deemed insufficient, the CyberSecDome consortium reserves the right to disqualify the applicant or terminate funding.

5.8.5 Non-Duplication of Funding

Applicants must declare that the activities proposed under the CyberSecDome Open Call are not receiving double funding from other EU or national programmes for the same scope of work. The goal is to ensure that the resources allocated for the project are used efficiently and to prevent overlapping financial support from multiple sources for the same activities.

5.8.5.1 No Double Funding

Applicants must declare that they are not receiving financial support for the same activities from:

- Horizon Europe or other EU research and innovation programmes.
- National or regional funding schemes that overlap with the objectives and activities of the CyberSecDome Open Call.

5.8.5.2 Grant Exclusivity:

The CyberSecDome grant should be the primary funding source for the proposed project activities. Applicants must ensure that any other grants or funding they receive are for separate activities that do not overlap with the scope and objectives of the CyberSecDome project.

5.8.5.3 Consequences of Non-Compliance:

- If it is discovered that an applicant is receiving double funding for the same activities, the applicant's project will be disqualified, and they will be required to return any funds already received under the CyberSecDome Open Call.
- The CyberSecDome consortium reserves the right to terminate the grant if double funding is identified at any stage during the project.

Applicants are expected to comply with these guidelines throughout the entire project duration. Regular audits and checks may be conducted to ensure compliance with the non-duplication of funding rules.

5.8.6 Audit and Verification Rights

To ensure compliance with the terms and conditions of the CyberSecDome Open Call, the CyberSecDome consortium and the European Commission reserve the right to audit

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

and verify all project-related activities. This includes financial records, technical progress, and any other documentation that supports the project's execution and alignment with the agreed-upon objectives.

5.8.6.1 Financial Audits

- The CyberSecDome consortium may conduct audits of the financial statements, project accounts, and expenditure records at any time during the project's duration or after its completion.
- Applicants must ensure that all eligible costs reported are in line with the guidelines of the **HORIZON EUROPE MGA** and the CyberSecDome Third-Party Funding Agreement (TPFA).
- Applicants must retain complete financial documentation, including invoices, payroll records, and receipts for all eligible expenses, for at least five years after the project is completed.

5.8.6.2 Project Audits

- In addition to financial audits, the CyberSecDome consortium may review the technical progress of the project to ensure it is meeting the defined milestones, deliverables, and Key Performance Indicators (KPIs).
- Applicants must submit regular progress reports as outlined in the **CyberSecDome Third-Party Funding Agreement (TPFA)** and make all relevant documentation available upon request.

5.8.6.3 On-Site Inspections

The CyberSecDome consortium and/or the European Commission may carry out on-site inspections of the applicant's premises or any location where project activities are being implemented.

5.8.6.4 Verification of Compliance:

- The applicant must comply with all relevant regulations, including those related to data protection (e.g., GDPR), environmental impact, ethical standards, and safety.
- If any discrepancies or violations are discovered, the CyberSecDome consortium may require corrective actions to be taken within a specified deadline.

5.8.6.5 Consequences of Non-Compliance:

- Failure to comply with audit and verification requirements, including the discovery of misreported costs, non-compliance with EU regulations, or other irregularities, may result in the termination of the grant.

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

- The consortium reserves the right to demand the return of any disbursed funds if the audit reveals non-compliance with the **CyberSecDome Third-Party Funding Agreement (TPFA)** or misuse of funds.

Applicants must adhere to these audit and verification rights throughout the project and post-project period. Maintaining transparency and accountability in financial and project reporting is essential to ensure continued funding and support.

5.8.7 Withdrawal or Termination of Funding

The CyberSecDome consortium reserves the right to withdraw or terminate funding under certain conditions if the applicant fails to meet the obligations outlined in the CyberSecDome Third-Party Funding Agreement (TPFA) or is found to be non-compliant with the terms of the CyberSecDome Open Call.

Funding may be withdrawn or terminated under the following circumstances:

- **Failure to Comply with CyberSecDome Third-Party Funding Agreement (TPFA):**
  - If the applicant does not meet the requirements outlined in the CyberSecDome Third-Party Funding Agreement (TPFA), including compliance with reporting requirements, deadlines, or adherence to data management plans, the CyberSecDome consortium may terminate funding.
  - Non-compliance with project deliverables, milestones, or Key Performance Indicators (KPIs) may also lead to funding withdrawal.
- **Fraudulent or Illegal Activity:**
  - If the applicant or any of its representatives are found to have engaged in fraudulent, unethical, or illegal activities during the proposal process or during project implementation, the funding will be immediately terminated.
  - Applicants must also avoid any involvement in criminal activities such as money laundering, terrorism financing, or other illegal financial practices.
- **Non-Performance or Poor Project Progress:**
  - Funding may be withdrawn if the applicant fails to deliver the project outcomes or does not make satisfactory progress toward the project's goals. Failure to meet milestones or significant delays in deliverables may be grounds for funding termination.
  - If the project does not demonstrate impact or if the quality of the deliverables is deemed insufficient, funding may be reduced or terminated.
- **Breach of Conflict of Interest or Double Funding Rules:**

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

  - If it is found that the applicant failed to disclose a conflict of interest, or if the applicant is receiving double funding for the same activities, the CyberSecDome consortium reserves the right to withdraw funding immediately.
  - Any undisclosed conflicts or violations of the non-duplication of funding clause will result in the termination of the grant and potential repayment of funds.
- **Risk Assessment:**
  - The consortium reserves the right to terminate funding if the project's risk profile, including financial or reputational risks, is deemed too high. This may occur if the applicant's financial capability is inadequate or if new risks emerge during the course of the project that compromise its viability.

Applicants must comply with all requirements and conditions throughout the project lifecycle. If the funding is withdrawn or terminated, the applicant may be required to repay any funds already received, depending on the severity of the non-compliance or breach of contract.