



AI-DRIVEN CYBERSECURITY FOR FINANCIAL SERVICE PROVIDERS

D1.1-PROJECT MANAGEMENT HANDBOOK

Lead Beneficiary	UBI
Work Package Ref.	WP1-Management and Coordination Activities
Task Ref.	T1.1-Administrative Coordination and Financial Management
Deliverable Title	D1.1-Project Management Handbook
Due Date	28/02/2026
Delivered Date	27/02/2026
Revision Number	1.0
Dissemination Level	Public (PU)
Type	Report (R)
Document Status	Final
Review Status	Reviewed
Document Acceptance	Acceptable
EC Project Officer	Rodica MORARIU

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH



The project funded under Grant Agreement No 101249596 is supported by the European Cybersecurity Competence Centre

DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

COPYRIGHT MESSAGE

This report, if not confidential, is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0); a copy is available here: <https://creativecommons.org/licenses/by/4.0/>. You are free to share (copy and redistribute the material in any medium or format) and adapt (remix, transform, and build upon the material for any purpose, even commercially) under the following terms: (i) attribution (you must give appropriate credit, provide a link to the license, and indicate if changes were made; you may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use); (ii) no additional restrictions (you may not apply legal terms or technological measures that legally restrict others from doing anything the license permits).

CONTRIBUTING PARTNERS

Partner Acronym	Role ¹	Name Surname ²
UBI	Lead Beneficiary	Louiza Kachrimani
FAIR	Reviewer	Fernando Ferreira
JRC	Reviewer	Konstantina Tripodi

REVISION HISTORY

Version	Date	Partner(s)	Description
0.1	29/01/2026	UBI	ToC Version
0.2	11/02/2026	UBI	1st Version for review
0.3	12/02/2026	JRC	Reviewed by JRC
0.4	19/02/2026	FAIR	Reviewed by FAIR
0.5	25/02/2026	UBI	Changes based on the review
1.0	27/02/2026	UBI	Final quality check and submission to the EU

¹ Lead Beneficiary, Contributor, Internal Reviewer, Quality Assurance

² Can be left void

LIST OF ABBREVIATIONS

Acronym	Definition
CA	Consortium Agreement
DoA	Description of Action
FS	Financial Statement
GA	Grant Agreement
PC	Project Coordinator
PMs	Personal Months
RTD	Research, Technology and Development
TC	Technical Coordinator
WP	Work package
PCT	Project Coordination Team
DM	Dissemination Manager
QRM	Quality and Risk Manager
IEM	Innovation and Exploitation Manager
ToC	Table of Contents

EXECUTIVE SUMMARY

The specific deliverable entitled “Project Management Handbook” provides the definition of the processes and mechanisms to be utilized and followed during the lifecycle of CyberAid project towards the successful execution of its tasks and achievement of its objectives. Its purpose is to identify the processes, the metrics, and the supportive documentation that are required and need to be defined and deployed so as to ensure the high-quality of CyberAid results and project management activities.

In the CyberAid project, complying with the project management procedures falls under the responsibility of the PC, as well as the WP leaders and Tasks leaders. Effective channels of internal communication have been established from M1 in order to exchange all the necessary information for the project implementation among the participants. The means for remotely conveying information for the CyberAid purposes range from e-mail communication through dedicated mailing lists and teleconferencing facilities to an internal collaboration space for document management and task management activities. Regarding the project meetings, an analysis of expectations and responsibilities has been performed, while a tentative schedule of project meetings for the whole implementation of the CyberAid project has been prepared.

The implementation aspects regarding co-creation and consultation mechanisms, official and internal reporting procedures, decision-making and conflict resolution processes to be applied during the CyberAid implementation have been defined in detail. Document control aspects regarding the documentation requirements, templates, naming conventions, and versioning have also been specified and agreed.

Finally, the deliverable provides information on the reporting process and the responsibilities and relevant deadlines of the partners.

TABLE OF CONTENTS

1.	Introduction	8
1.1	Objectives of the Deliverable	8
1.2	Structure	8
2.	Consortium Composition, contacts and management structure.	9
2.1	Consortium and participants	9
2.2	Management Structure	9
2.3	Bodies and Main roles	10
2.3.1	Project Coordination Team	10
3.	Implementation Aspects	11
3.1	Decision Making	11
3.2	Conflict Resolution	11
4.	Reporting Procedure and Payment Arrangements	11
4.1	Reporting Procedures	12
4.1.1	Internal Activity Report	12
4.1.2	Project Periodic Report	12
4.1.3	Project final report	13
4.2	Payment Schedule	13
5.	Communication among partners	13
5.1	Meetings	13
5.2	Mailing lists	14
5.3	Project collaborative space-Infrastructure and Repository	15
6.	Deliverable Submission and Quality Management	17
6.1	Document Control Management	17
6.2.1	Documentation Requirements	18
6.2.2	Naming Conventions and Versioning	18
6.2.3	Deliverables submitted to the EC	19
6.2.4	Project Presentations	19
6.2.5	Meeting Agenda	19
6.2.6	Meeting Minutes	19
6.2.7	Reviewed documents and Internal Audit Reports	19
6.2.8	Security Levels	20
6.2.9	Code of Conduct	20
7.	Funding Acknowledgement	21
7.1	EU Acknowledgement in Dissemination Results	21
7.2	EU Acknowledgement in scientific papers	21
8.	Management of Knowledge and Intellectual Property	22

9. Conclusions 22

10. Annexes.....23

10.1 Deliverable Template 23

10.2 Presentation template 24

10.3 Minutes Template 25

10.4 Interim Reporting Template 26

LIST OF FIGURES

Figure 1- Project Partners 9

Figure 2-CyberAid Microsoft SharePoint Space.....15

Figure 3-CyberAid GitLab Space 16

Figure 4-CyberAid Slack space.....17

Figure 5-EU Logos.....21

Figure 6-Project Logo 21

LIST OF TABLES

Table 1-Project Meetings 14

1. INTRODUCTION

1.1 Objectives of the Deliverable

The purpose of the present deliverable entitled “Project Handbook” is to provide a quick overview of the project management structure and the most relevant managerial aspects to be followed, based on a proper implementation of the general mechanisms of work and setting the rules and responsibilities of the CyberAid consortium. The objective is to ensure a high-quality progress of the work during the project lifetime. This includes the production of the deliverables and other project outcomes, the mechanisms for their submission and the internal review process, and the communication means among partners (i.e., meetings, mailing lists, project collaborative space).

In this context, the present deliverable aims to fulfil the following main objectives:

- Provide a clear overview of the project management structure, including roles, responsibilities, and decision-making bodies within the CyberAid consortium.
- Define the general mechanisms of work, ensuring a common understanding of procedures, workflows, and collaboration principles among all partners.
- Establish rules and responsibilities to support effective coordination, accountability, and compliance throughout the project lifecycle.
- Describe the deliverable production and submission process, formats, and responsibilities.
- Define communication and collaboration mechanisms, such as meetings, mailing lists, and the project’s collaborative workspace, to facilitate efficient information exchange.

1.2 Structure

The structure of the Project Handbook is as follows:

1. Consortium Composition, Contacts and Management Structure: This section outlines the organizational framework guiding the project, including roles, responsibilities, and governance mechanisms.
2. Implementation aspects: This section presents the process for decision-making and conflict resolution.
3. Reporting Procedure and Payment Arrangements: This section details the procedures for progress reporting, financial management, and payment schedules.
4. Communication among Partners: This section describes the channels and methods for effective internal communication to ensure seamless information flow among project participants.
5. Deliverable Submission and Quality Management: This section introduces processes for submitting project deliverables and the document control management procedure.
6. Management of Knowledge and Intellectual Property: This section addresses the strategies for managing project knowledge and intellectual property rights.

Additionally, the annexes provide supplementary information and templates to support the main sections of the document.

By following the guidelines and procedures outlined in this handbook, the CyberAid project aims to achieve its objectives with a high degree of efficiency, quality, and collaboration among all participants.

2. CONSORTIUM COMPOSITION, CONTACTS AND MANAGEMENT STRUCTURE

2.1 Consortium and participants

Official contact information for each Project Participant is included in the CyberAid Grant Agreement. The full list of project participants, along with subscription to mailing lists is maintained as a living document in the CyberAid Project Repository as a document restricted to the consortium. Partners are responsible to inform about any modification of their representatives both the Project Coordinator and the Project Coordination Team or the respective WP leader, who will be responsible for informing the rest of members (if necessary).

Partners of the project:



Figure 1- Project Partners

2.2 Management Structure

The project management in CyberAid will guarantee transparency and commitment to all engaged partners and thus, facilitate an unobstructed and successful project evolution. The overall project management of CyberAid will comply with the following two major principles, namely the: (1) Principle of creating an integrated project structure incorporating technical, scientific and partner coordination as well as issues of commonplace business operation, based on the methodology of the Project Management Institute (PMI) and supported with state of-the-art management instruments; and (2) Principle of achieving agreement upon all partners and ensuring that decision-making takes place as close as possible to the level of implementation, while escalating issues when necessary, and safeguarding the reliable agreements in order to protect the intellectual property of all partners.

The project structure is designed to handle the most important aspects of management, namely decision-making, IPR policy, technical and administrative management, advisory functions and assessment. The overall management of the project will be facilitated by a consistent and formal approach. In any event, a detailed internal Project Plan will be defined in the preliminary stage of the project, to support the contractual Work Plan and to form the basis of the administrative structures and procedures to be used. The reporting lines and decision-making procedures are described in detail in the following sections.

The primary aim of this management structure is to be capable of responding to the needs of an Innovation Action without being intrusive or costly. The building-in of flexibility was one essential aspect while defining this structure.

2.3 Bodies and Main roles

Description and duties of these entities are fully described in the Grant Agreement and are thus only briefly reported below.

2.3.1 Project Coordination Team

CyberAid Project Coordination Team (PCT) is responsible for the planning, execution and controlling of the project. More specifically the PCT encompasses the following activities: (A) Administration and scientific coordination activities; (B) Implementation of all action plans; (C) Establishing a budget and schedule-controlling system; (D) Implementation of a quality assurance system; (E) Providing clear guidance on Intellectual Property issues; (F) Developing and maintaining a communication and reporting attitude; (G) Creation of efficient team structures to minimize the number of meetings while being flexible. The following roles constitute the PCT:

1. The Project Coordinator (PC) - Mrs. Louiza Kachrimani (UBI), will be responsible for the overall management of the project and will be the single point of contact with the EC. The PC coordinates all the communications within the partners to ensure progress and quality of the work and provides the Project Officer with technical, managerial, and financial information. Indicative administrative tasks of the PC include the supervision of the overall project progress, the preparation of the General Assembly meetings, the CA coordination, the supervision of the distribution of EC payments to each beneficiary, the preparation of the review meetings and the project's representation. In order to fulfil her tasks, the PC uses the resources of project management office team.
2. The Technical Coordinator (TC) – Mr. Ioannis Ledakis, will be responsible for the overall scientific and technical management and progress of the project and has the responsibility to coordinate the overall technical progress, to facilitate the alignment of the technical WPs with users' requirements, to consolidate the technical reports and review of technical deliverable and to coordinate the validation pilots and assessment.
3. Pilots Operation Manager- Mr. Giorgio Da Bormida (GFT) will be responsible for all CyberAid pilots and in contact with all pilot organisation leaders.
4. The Quality and Risk Manager (QRM) – Mr. Michele Canteri (GFT) will be responsible for the implementation of quality procedures identified in this deliverable and will oversee the quality assurance of deliverables. He will also act as risks evaluator.
5. The Communication Manager (DM) – Mrs. Stamatia Moniou (INNOV) will be responsible for monitoring and coordinating the communication and dissemination activities of the project and managing the collaboration with various communities and external stakeholders.
6. Innovation and Exploitation Manager (IEM)- Dr. Ioannis Soldatos (INNOV) will manage and execute the overall exploitation plan of the project and be responsible for the project's results scientific and technical exploitation.

Another important body of the project is the Technical Committee, which is expected to be the project's technology driving force. The Committee is in charge of supervising the project's technological progress/achievements and submitting proposals to the Coordinator and PCT on all relevant technical issues. The committee is led by the technical coordinator, UBI, and it consists of the technical partners.

3. IMPLEMENTATION ASPECTS

3.1 Decision Making

Decisions regarding the project implementation will normally be taken by the team members upon reaching consensus with the WP leaders. Typically, agreement will be reached first by informal contact, followed by official confirmation via electronic mail, letter or agreed written minutes. In case there is a dispute between two or more team members, a conflict resolution procedure must be followed, as presented in the specific document.

For important issues, the agreement may take the form of a short report that needs to be signed by the PCT. Non-technical factors such as resource allocation and contractual terms will also need to be agreed and documented in writing.

The key driver of the decision-making procedures is the description of work (DoA) to be performed as stated in the Consortium Agreement (CA), the DoA, and the Quality Plan, and as regularly communicated within the consortium. Transparency of the implementation decisions and actions will be achieved by adequate communication of the emerging issues in project meetings and e-mail communications.

3.2 Conflict Resolution

Generally, technical issues or conflicts within the contractual commitments that do not involve any contract, budget, resource allocation or overall project focus changes will be discussed at work package level first.

If the decision reached between team members is unacceptable by other partners, the conflict will be resolved according to a conflict resolution procedure which can be summarized in the next steps:

1. The team members involved in the implementation of the WP will inform the WP leader for the emerging conflict.
2. The WP leader will decide whether the issue needs to be discussed in a teleconference or a dedicated WP Meeting. The WP Leader will inform the PC for the planned actions.
3. The result of the teleconference or the meeting will be communicated to the PC.
4. If no consensus has been reached so far, the PC will contact the responsible persons and will try to resolve the conflict.
5. In case that the disagreement remains, the issue will be escalated in the PCT. The decision that will be taken at this level will be considered as the final resolution of the issue.

4. REPORTING PROCEDURE AND PAYMENT ARRANGEMENTS

Project reporting is the procedure used by the European Commission (EC) to monitor, assess, and follow up on funded projects. As such, it is of utmost importance, as it directly influences the project's overall evaluation with the EC. It is important to remark that the project reporting is a responsibility of the whole Consortium, and every partner must be actively involved in it. The PC is responsible for periodically

gathering the information and reports from the different partners and consolidating them before sending them to the EC.

There are two types of reporting documents, including technical and financial information: the Project Periodic Report and the Internal Activity Report. The Project Periodic Report refers to the official report that must be submitted to the EC according to the EC guidelines and templates. The Internal Activity Report refers to internal documents that will be used as control measures to effectively monitor the technical and economic progress of the CyberAid project. The Internal Activity Reports will also feed the official reports.

4.1 Reporting Procedures

4.1.1 Internal Activity Report

CyberAid Internal Activity Reports have to be prepared by consortium partners and provided to the PC two times per year (every 6 months). An Internal Activity Report shall contain: (a) Technical Information about the WP progress as provided by the respective WP leaders, (b) Effort Information as all partners will be requested to provide a breakdown of the effort spent in the related semester, per WP in comparison to the planned effort.

The procedure to be followed is:

At the end of the 6-month period, the PC will send to the consortium an email with instructions and the template to be filled in;

Each Partner has to fill in:

- a. short description of work done (per WP and Task),
- b. achievements and results,
- c. problems occurred,
- d. brief overview of planned activities for upcoming semester
- e. overview of dissemination/exploitation/cooperation/standardization activities
- f. an estimation of resources spent (PMs) per WP in the respective reporting semester against the actual total PMs per WP

The partners send their report to the PC within 30 days after the closure of the period.

4.1.2 Project Periodic Report

During the CyberAid project, two official Project Periodic Reports must be submitted to the EC by the PC, covering the following reporting periods: a) Reporting Period 1 (M1–M18): 01/01/2026 – 30/06/2027, b) Reporting Period 2 (M19–M36): 01/07/2027 – 31/12/2028.

The reports shall be submitted to the EC for each reporting period within 60 days after the end of the period under assessment. The delay in the submission of these reports may cause the postponement of part of the next payment to be received by the partner until the next reporting period. The technical part will be managed through corresponding Project Periodic Reports. The PC is in charge to prepare the specific reports based on the information provided through Internal Activity Reports.

The financial status of the project and costs incurred during the period must be communicated to the EC through meticulously prepared Financial Statements (FS) in order to justify the incurred costs and expenses and qualify for the next/final payment. Each consortium partner has to upload financial information to the EC participant portal (ECAS) based on cumulative information obtained from the Interim Activity Report.

The procedure to be followed is:

- The PC will ask the partners to generate their individual FS in the EC Participant Portal to officially declare the costs incurred for the reference period;
- Each partner will complete the FS with the costs incurred during the period;
- Each partner will submit and digitally sign the FS. This signature will be done by the Project Financial Signatory appointed; and
- The Coordinator will submit the financial report to the EC;

4.1.3 Project final report

In addition to the final Periodic reports, a Final Report has to be submitted by the coordinator to the EC 60 days after the end of the last reporting period.

4.2 Payment Schedule

The payment schedule, which contains the transfer of pre-financing, interim and final payments to Parties, will be handled according to the following:

Given that the amount of the pre-financing payment is 3.999.918,09€, it will be paid to Parties after receipt from the Funding Authority and the Parties have signed the CA.

For the payment of the balance (final payment); the provisions of the Grant Agreement will be followed.

Costs accepted by the Funding Authority, pertaining to interim and final payments, will be paid to Parties after receipt from the Funding Authority within 30 days and in conformity with the provisions of the Grant Agreement.

Payments shall be made following confirmation of each Party's bank account details, and after the signature of both CA and Financial identification form by the partners.

The Coordinator is entitled to withhold any payments due to a Party identified by a responsible Consortium Body to be in breach of its obligations under this CA or the GA or to a Beneficiary which has not yet signed this CA.

The Coordinator is entitled to recover any payments already paid to a Defaulting Party. The Coordinator is equally entitled to withhold payments to a Party when this is suggested by or agreed with the Funding Authority.

5. COMMUNICATION AMONG PARTNERS

Efficient communication and collaboration structures are essential for the success of the project. Since all project partners are distributed across European member states, the centerpiece of the overall project communication will be a protected online collaboration platform, offering to each partner independent access to important documents, code, meeting agendas, supporting materials, individual to-do lists and other miscellaneous project information.

5.1 Meetings

Regular and ad-hoc meetings will be held during the project lifecycle, including:

Project Plenary Meetings held every 6 months in order to ensure that all procedures are understood and implemented in the proper way. The PC is responsible for the meeting formation (agenda of the meeting)

and the communication of the meeting details (time, place) at least 2 weeks before the date of the meeting, in order to allow time to the participants for the scheduling and preparation of the necessary information for the meeting.

Technical Partners Meetings are held per case if required. Those meetings will be organised by the TC.

Bi-weekly WPs meetings, monitored by WP leaders. WP leaders in alignment with Task leaders should present the progress of their WP as well as any open issue of admin, financing nature etc.

Monthly meetings for all active WPs (PCT Meetings): Each WP leader will propose the meeting schedule according to his WP needs at least 1 week before the date of the meeting and coordinate the necessary actions among the involved partners for the implementation of the WP activities. Each WP leader will communicate the final agenda of the meeting at least 1 day before the meeting date.

A tentative table of the project meetings is available below.

Table 1-Project Meetings

Event	Date	Place
Kick-off meeting	January 2026	Athens
2nd Plenary Meeting	June 2026	TBD
3rd Plenary Meeting	January 2027	TBD
4th Plenary Meeting	June 2027	TBD
5th Plenary Meeting	January 2028	TBD
6th Plenary Meeting	June 2028	TBD

5.2 Mailing lists

Effective channels of internal communication have been established from M1 in order to exchange all the necessary information for the project implementation, such as deliverables and relevant documentation. Internal communication channels are also used for exchanging messages.

A set of e-mail distribution lists have been created to facilitate the communication flows within the different bodies of the consortium. In particular, the following mailing lists have been created:

- general@cyberaidproject.eu
- wp2@cyberaidproject.eu
- wp3@cyberaidproject.eu
- wp4@cyberaidproject.eu
- wp5@cyberaidproject.eu
- wp6@cyberaidproject.eu
- wp7@cyberaidproject.eu

Subscription of each project member to a specific mailing list is managed and maintained by the PC. The updated subscription list is available through the CyberAid Project Repository. Each consortium partner is responsible for informing the PC whether any modification of their representatives is needed, and the PC will be responsible for keeping the distribution lists updated and informing the rest of the members.

5.3 Project collaborative space-Infrastructure and Repository

UBI deployed and will operate the internal Documents and Electronic Material Repository in the following URL: <https://ubitechu.sharepoint.com/sites/CyberAid> using **Microsoft SharePoint**

This repository includes:

- WPs documentation (technical documentation, deliverables)
- Meeting minutes and agendas
- Dissemination materials
- Legal and Administrative documents
- Any other relevant project documents

This repository will be a central location where all project partners can easily access and share important documents. UBI has provided access to all partners.

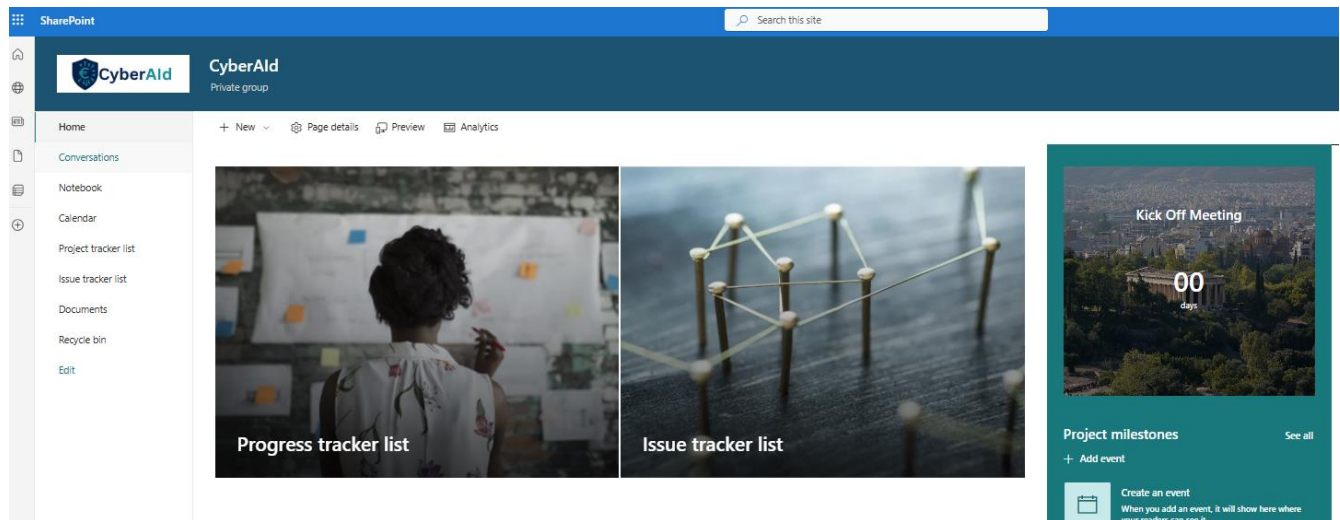


Figure 2-CyberAid Microsoft SharePoint Space

A brief summary of the documentation organization and content of the CyberAid Project Repository with respect to the Document Management System:

- 01 - Administrative Documents – it contains the created documents' templates to be utilized, as well participants' contacts details and reporting folder.
- 02 - Legal Documents: Contractual documents, containing the Grant Agreement with EC and its annexes and the CA with its annexes. Moreover, it encloses a financial reporting folder that is created where all financial related documents will be stored for the CyberAid reporting periods.
- 03 – Work Packages: A folder per Work package is created. In each WP folder, separate folders per Deliverable are also created. In each Deliverable folder, the consortium will store the material files required, the various contributions, the deliverable's editing versions, the review reports, as well as the final draft and the submitted deliverable to the EC.

- 04 - Submitted Deliverables: The specific folder contains the list of the PDF files of the deliverables as these will be officially uploaded to ECAS System.
- 05 – Meeting + Telcos: The specific folder contains the files that refer to Meeting Agendas, Meeting Minutes, as well as Meeting Partners’ Presentations. Furthermore, it contains the folder structure to support the storage of all Teleconferences Presentations and Minutes describing the decisions made and action plans produced.
- 06 - How To’s: it contains the User Guide for CyberAid repository. Furthermore, it will contain any other How-To’s or Manuals that will be produced within the frame of the project

GitLab will be also used as the central platform for collaborative software development and project coordination where all partners can jointly manage source code, track tasks and milestones, document technical results, and ensure quality through automated testing and continuous integration

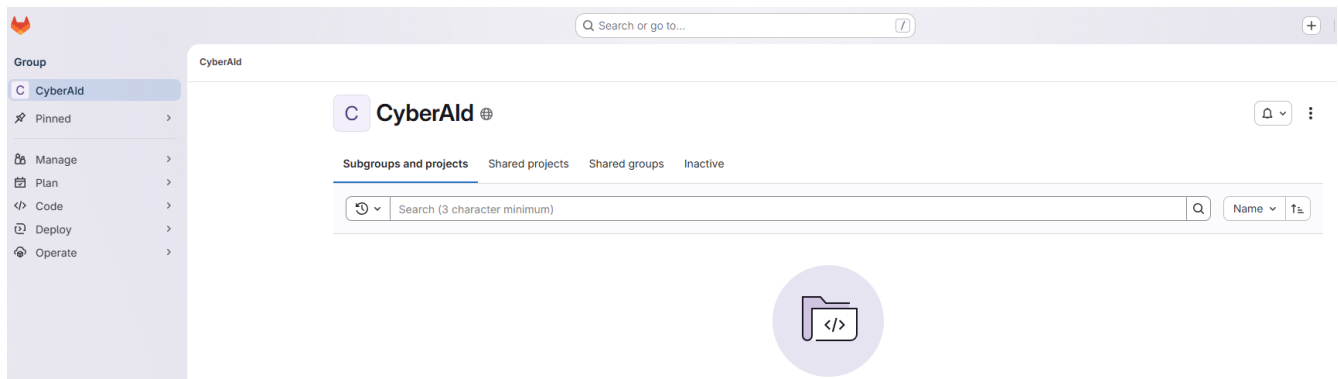


Figure 3-CyberAid GitLab Space

Slack will be also used for enabling efficient day-to-day collaboration among consortium partners. It supports structured discussions through dedicated channels aligned with work packages, tasks, and governance bodies, facilitating timely information sharing and quick decision-making.

☆ #all-cyberaid

Messages Add canvas +

Everyone's all here in #all-cyberaid

Share announcements and updates about company news, upcoming events, or teammates who deserve some kudos. ★

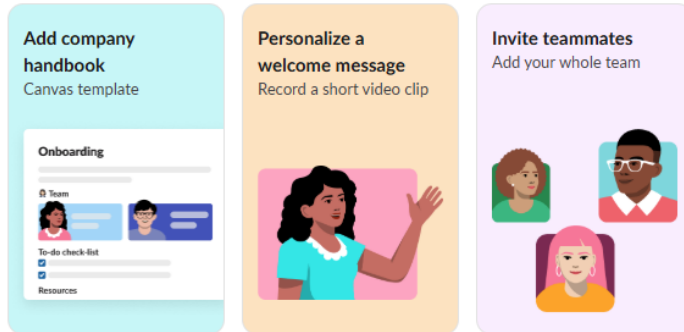


Figure 4-CyberAid Slack space

6. DELIVERABLE SUBMISSION AND QUALITY MANAGEMENT

The different technical objectives set for the project have their correspondence within the work packages and defined tasks. Compliance with these technical objectives is evident by on-time delivery of the corresponding Deliverables. Each deliverable is assigned to Lead Beneficiary partner, who will be responsible for its timely elaboration. Every Lead Beneficiary is fully responsible for the deliverable's quality and is required to maintain adequate control of the participants' contributions.

The deliverables shall be submitted to the EC in English, by electronic means (in pdf format in the Participants Portal) or in any other format only if required by EC. The appropriate and updated deliverable template can be found in the CyberAid Project Repository.

All the deliverables must be finalized and submitted to the EC within the deadlines defined in Annex I of the Grant Agreement.

The process to be followed for the deliverable preparation and submission will be documented in D1.2.

6.1 Document Control Management

The Document Control Management deals with the preparation of template documents, the identification and the tracking of changes related to draft and final versions of documents circulated among the partners. The PC is responsible for the necessary assessment of deliverables, while the TC will be responsible for the overall monitoring of the entire document control and configuration management activities described in this section.

Type	Responsible	Template
Internal Project Presentation	All partners	Project Presentation Template
Meeting Agenda	Project Coordinator	Meeting Agenda Template

Meeting Minutes	Project Coordinator & Technical Coordinator	Meeting Minutes Template
Reviewed Document	All partners	A new version with track changes on the original version
Internal Review Report	All partners	Internal Review Report Template
Final Activity Report	Project Coordinator / WP Leaders	As per Grant Agreement and Commission guidelines
Final Management Report	Project Coordinator	As per Grant Agreement and Commission guidelines
Financial Statement	All Partners	As per Grant Agreement and Commission guidelines
Consolidated Financial Statement	Financial Administrator	As per Grant Agreement and Commission guidelines

6.2.1 Documentation Requirements

In the span of the CyberAId project, a set of deliverables and relevant documented results are anticipated as depicted in the following tables. Such documents will be sent by e-mail and will be uploaded to the restricted CyberAId document repository, if they comply with the following standards:

- Word Processor: Microsoft Word 2007 and higher,
- Spreadsheet: Microsoft Excel 2007 and higher,
- Presentations: Microsoft PowerPoint 2007 and higher.

All files should be scanned for potential viruses before issued and screened on receipt. If an acknowledgement is requested, an explicit request should be included by the sender at the top of the message (e-mail, fax, etc.)

6.2.2 Naming Conventions and Versioning

Document configuration management will be ensured through tracking the versions and the history of changes within the various project documents, such as:

- Deliverables (as stated in the deliverables list in the DoA);
- Presentations of the project results.
- Meeting agenda and minutes; and
- Internal audit reports and reviewed deliverables, including the corrective actions taken.

Document versioning will be tracked for each deliverable in a separate table that describes the document's versions and the reasons for changes/updates.

6.2.3 Deliverables submitted to the EC

Name	CyberAid Deliverable Code_[Deliverable Title]_vA.BB
Where	A: Major version of the deliverable (Submission to Commission)
	BB: Minor version of the deliverable for updates during the preparation phase
Examples	CyberAid_D1.1_Project Management Handbook_v1.00 (for submission to the Commission)
	CyberAid_D1.1_Project Management Handbook_UBI_v0.30 (for internal updates and submission for internal review)

6.2.4 Project Presentations

Name	CyberAid_[Purpose] or [WP Number]_[Partner]_vA.BB
Where	A: Major version of the presentation (Presentation in the event / workshop)
	BB: Minor version of the presentation for updates during the preparation phase
Examples	CyberAid_WP1_UBI_v1.00

6.2.5 Meeting Agenda

Name	CyberAid_[Meeting Number] Meeting_Agenda_[Place]_vA.BB
Where	A: Major version of the meeting agenda
	BB: Minor version of the meeting agenda for updates during the preparation phase.
Examples	Place: Venue city
	CyberAid_KOM Agenda_Athens_v1.00 (final version) CyberAid_KOM Agenda_Athens_v0.10 (for internal updates and submission for internal review)

6.2.6 Meeting Minutes

Name	CyberAid_[Meeting Number] Meeting_Minutes_[Place]_vA.BB
Where	A: Major version of the meeting minutes
	BB: Minor version of the meeting minutes for updates during the preparation phase Place: Venue city
Examples	CyberAid_KOM Minutes_Athens_v1.00 (final version)
	CyberAid_KOM Minutes_Athens_v0.10 (for internal updates and submission for internal review)

6.2.7 Reviewed documents and Internal Audit Reports

Name	CyberAid_[Deliverable Code] -[TR/QR]_[Partner/Expert]_vA.BB
------	---

Where Major version of the deliverable / internal audit report

BB: Minor version of the deliverable / internal audit report for updates during the preparation phase

TR: Technical Reviewed document

QR: Quality Reviewed document

Examples CyberAld_D1.1-TR_UBI_v0.31 (Technical Reviewed Document from UBI)
CyberAld_D1.1-TR_UBI_v0.31-Internal Audit (Review report from UBI)
CyberAld_D8.1-QR_UBI_v0.41 (Quality Reviewed Document from GFT)

6.2.8 Security Levels

Abbreviation	Type	Security Level
PU	Public	Fully Open
SEN	Sensitive	limited under the conditions of the Grant Agreement
EUI	EU Classified	EU classified (EUCI) under Decision 2015/444: • RESTREINT-UE/EU-RESTRICTED (R-UE/EU-R), • CONFIDENTIEL-UE/EU-CONFIDENTIAL (CUE/EU-C), • SECRET-UE/EU-SECRET (S-UE/EU-S)
Reviewed Document	All partners	A new version with track changes on the original version

As a rule, the European Commission Services have free access to all the Deliverables and Internal Deliverables produced by the Project.

6.2.9 Code of Conduct

CyberAld partners are expected to jointly develop new ideas, concepts, and architectures, as well as to pursue, jointly or individually, relevant opportunities for dissemination and exploitation of the project results. Therefore, to guarantee open and frank collaboration among the consortium members, namely when this involves original contributions and information subject to some level of confidentiality, the following principles shall be observed:

- The partners shall comply with the rules set by Annex II to the Contract (General Conditions) and by the CyberAld Consortium Agreement, in relation to:
 - o The Intellectual Property Rights (IPR), regarding any original contribution or background knowledge brought in by any member; and
 - o The IPR regarding any new knowledge (forward knowledge) generated in the framework of CyberAld because of any cooperative activity.
- In all forms of use of the mentioned knowledge, proper recognition to all original contributors should be made, namely through:

o Proper references in publications. When the referenced piece of knowledge has been published, standard referencing rules should apply. In case of draft ideas included in working documents, a reference to the author and corresponding document should be made; and

o Otherwise, in the case that there is no written reference, a note stating: "personal communication in the framework of the CyberAid project" can be used (identifying the contributor)

- Similar rules should be observed when using copies of slides that include substantial original ideas (figures or text).

- When reporting RTD results, Deliverables and Working Documents will contain a list of the contributing partners, intended as individuals of the involved organizations who have provided contributions to the document.

7. FUNDING ACKNOWLEDGEMENT

7.1 EU Acknowledgement in Dissemination Results

Any dissemination of results must display the EU emblem; thus, the CyberAid logo will be present on all materials related to communication, together with the EU emblem, a direct statement on the funding source and the Grant Agreement number.

The following logos should be used:



Figure 5-EU Logos



Figure 6-Project Logo

The following acknowledgement should be used:

“The project funded under Grant Agreement No 101249596 is supported by the European Cybersecurity Competence Centre”

7.2 EU Acknowledgement in scientific papers

Partners who proceed with scientific publications showcasing work implemented in the framework of the CyberAid project should include the following acknowledgement:

The work presented in this paper is carried out in the context of the CyberAId project - “AI-Driven Cybersecurity For Financial Service Providers”; and has been co-funded by European Cybersecurity Competence Centre under Grant Agreement No. 101249596

8. Management of Knowledge and Intellectual Property

The management of knowledge and intellectual property (IP) will be conducted in strict adherence to the Digital Europe contract template and the associated contractual conditions. This encompasses a range of issues, including but not limited to the ownership and protection of intellectual property, the dissemination of research findings, and the granting of access rights.

Ownership and Protection: The CA, signed by all project partners, details how intellectual property rights are allocated and protected throughout the project. It specifies how discoveries and innovations will be owned and managed to ensure proper protection and exploitation.

Dissemination of Knowledge: The agreement outlines procedures for sharing research results and other project outputs with the public and relevant stakeholders, in compliance with Digital Europe guidelines. This includes guidelines for publishing results, presenting findings at conferences, and other forms of dissemination.

Access Rights: The terms for accessing and using knowledge and IP generated during the project are clearly defined. This includes conditions under which partners can access each other's IP, as well as terms for any third-party access. The Grant Agreement (GA) plays a critical role in monitoring and ensuring that these conditions are implemented effectively. It will oversee compliance with the contractual stipulations set out in both the Digital Europe contract and the Consortium Agreement, addressing any issues that arise and ensuring that all partners adhere to the agreed-upon terms.

By closely following these guidelines, the project aims to protect its innovations, foster collaboration, and facilitate the effective dissemination of its findings, all while safeguarding the interests of all parties involved.

9. Conclusions

In conclusion, the "Project Management Handbook" for the CyberAId project has meticulously outlined the procedures, communication channels, and quality assurance mechanisms necessary for the project's success. The comprehensive management framework ensures that all participants are aligned with the project's objectives and equipped with the tools and processes required for efficient execution. By establishing clear guidelines for co-creation, consultation, decision-making, and conflict resolution, the handbook fosters a collaborative and transparent environment. Overall, the structured approach detailed in this management handbook will be instrumental in achieving the CyberAId project's goals and delivering impactful results.

10. ANNEXES

10.1 Deliverable Template



AI-DRIVEN CYBERSECURITY FOR FINANCIAL SERVICE PROVIDERS

DX.Y – TITLE OF THE DELIVERABLE

Lead Beneficiary	Partner Acronym
Work Package Ref.	WPX – Reference Work package Name
Task Ref.	TX.Z – Reference Task Name
Deliverable Title	DX.Y – Title of the Deliverable
Due Date	yyyy-mm-dd
Delivered Date	yyyy-mm-dd
Revision Number	M.N.
Dissemination Level	Public (PU) or Confidential (CO)
Type	Report (R) or Other (ORDP) or ETHICS
Document Status	Draft or Release
Review Status	Internally Reviewed and/or Quality Assurance Reviewed
Document Acceptance	WP Leader Accepted and/or Coordinator Accepted
EC Project Officer	Rodica MORARIU

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH



Co-funded by
the European Union



The project funded under Grant Agreement No 101249596 is supported by the European Cybersecurity Competence Centre

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

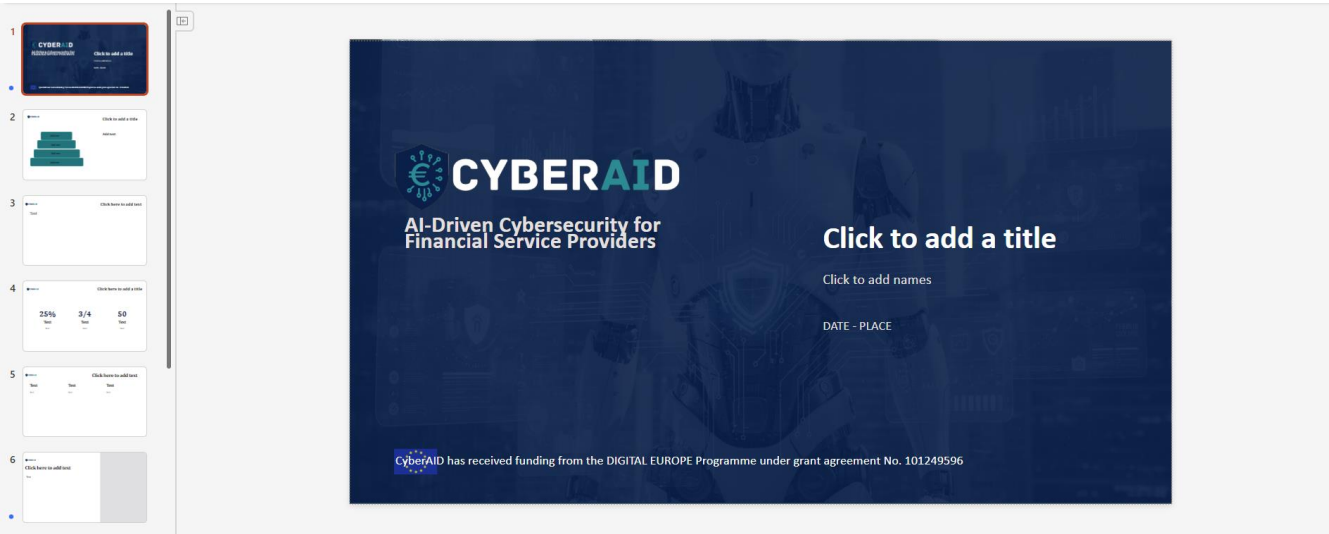
DISCLAIMER

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the EASME nor the European Commission is responsible for any use that may be made of the information contained therein.

COPYRIGHT MESSAGE

This report, if not confidential, is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0); a copy is available here: <https://creativecommons.org/licenses/by/4.0/>. You are free to share (copy and redistribute the material in any medium or format) and adapt (remix, transform, and build upon the material for any purpose, even commercially) under the following terms: (i) attribution (you must give appropriate credit, provide a link to the license, and indicate if changes were made; you may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use); (ii) no additional restrictions (you may not apply legal terms or technological measures that legally restrict others from doing anything the license permits).

10.2 Presentation template



10.3 Minutes Template

[illegible]

10.4 Interim Reporting Template



AI-Driven Cybersecurity for Financial Service Providers

GA No: 101249596

Beneficiary: 1 UBI

WP	Start Month	End Month	Partner Effort (according to GA)	Partner's Effort Distribution Planning (per semester and work-package)						PLANNED TOTAL	DIF from GA Effort
				Semester S1 (M1-M6)	Semester S2 (M7-M12)	Semester S3 (M13-M18)	Semester S4 (M19-M24)	Semester S5 (M25-M30)	Semester S6 (M31-M36)		
WP1	1	36									0,00
WP2	1	36									0,00
WP3	3	32									0,00
WP4	3	32									0,00
WP5	3	34									0,00
WP6	6	36									0,00
WP7	1	36									0,00
Total			0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00