MANAGEMENT HANDBOOK

CYBERAGENT 10.2023

Co-funded by the European Union

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

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 Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Work Package 1: Project management

Deliverable 1.1: Management handbook

Leader of WP1 and deliverable 1.1 – VU

CONTENT

ABBREVIATIONS

EC – European Commission

EVM – Ecosistemas Virtuales Y Modulares sl

HACKERU– Hackeru Polska Spolka z Ograniczona Odpowiedzialnoscia

HEI – a Higher Education Institution

Moisil Buzau – Liceul Tehnologic Grigore c Moisil

MSM – Monitoring and steering meetings

OLEMISEN – Olemisen Balanssia RY

PRIOS – Prios Kompetanse AS

Project – CyberAgent project

QMC – Quality Monitoring Committee

QMM – Quality Management and Monitoring

SC – Steering Committee

SME – Small and medium enterprise

TeknoparkMTAL – Ministry of National Education

VET – Vocational education and training institution

VU – Vilnius university

Women4Cyber – Women4Cyber Mari Kert - Saint Aubyn Foundation

WP – Work Package of the Project

LIST OF TABLES

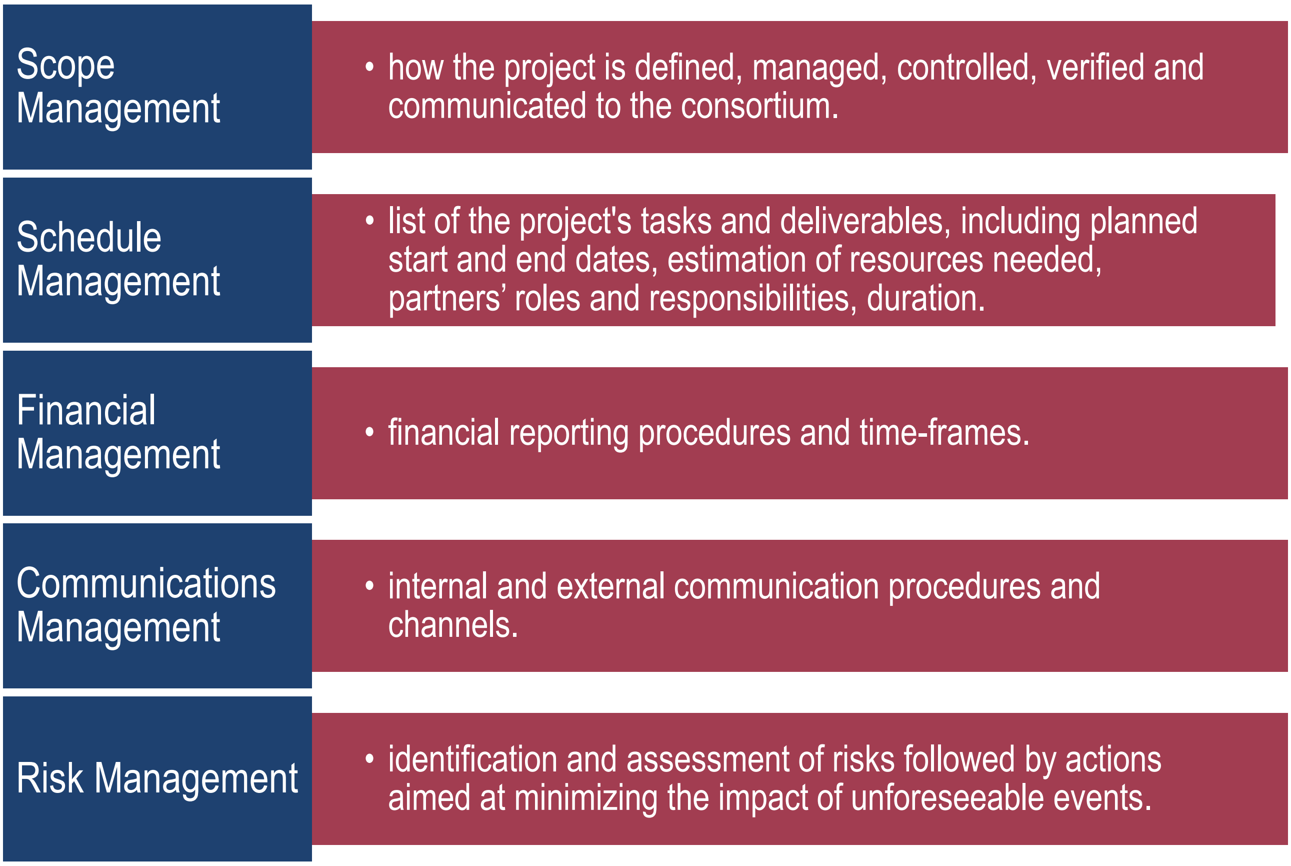
LIST OF FIGURES

INTRODUCTION

The aim of this Management handbook is to define the structure and content management to be used by CyberAgent project. The document is intended to ensure proper and efficient project management and efficient organization of Project activities, role of Partners, risk management, monitoring the Project's performance, implement the Project results in a quality manner using the resources foreseen in the Project application and ensure proper and efficient financial management, ensure effective communication and cooperation between the Partners and the flow of information from the Coordinator to the EC.

The Project management plan is presented in this handbook and includes the following sections: Scope Management, Schedule Management, Financial Management, Communications Management, Risk Management.

Figure 1: Project management plan structure



Scope Management
- how the project is defined, managed, controlled, verified and communicated to the consortium.

Schedule Management
- list of the project's tasks and deliverables, including planned start and end dates, estimation of resources needed, partners' roles and responsibilities, duration.

Financial Management
- financial reporting procedures and time-frames.

Communications Management
- internal and external communication procedures and channels.

Risk Management
- identification and assessment of risks followed by actions aimed at minimizing the impact of unforeseeable events.

The Management handbook is prepared based on the Grant agreement and Partnership agreement and cannot contradict them. This handbook is extended and supplemented by:

- The Quality Assurance and Monitoring Plan (QAMP) (D1.3. Deliverable)
- Dissemination & Communication Strategy (D6.1. Deliverable)
- Guidelines for Establishing a Knowledge Committee (D.2.1 Deliverable)

Detailed information about Project objectives, activities, task leaders, Project plan, deliverables and budget are given in the Grant Chart and Partnership agreement signed by CyberAgent partners. Hence, management refers to those documents regarding detailed information and focuses on Project management issues.

The Coordinator of the Project CyberAgent is Vilnius University (VU), which acts as the grant holder of this Project proposal. The Coordinator will work in collaboration with the named contact persons for the Project in the partnering countries. A coordinator is necessary and serves the whole Project partnership in keeping the Project plan together and maintaining the network and contacts. VU is responsible for meeting the entirety of the Project's obligations towards the EC.

The entire implementation of the Project will be accompanied by on-going monitoring and evaluation processes starting from the beginning of the Project and continuing until the end of the three-year-period. The results of each activity will be compared to the concrete objectives and targets described in the proposal as well as to the indicators and detailed success and quality criteria developed during the first meeting.

VU and OLEMISEN will lead Work Package 1. VU will be responsible for the effective running of the Project what includes the communication with the EC, administration of resources, Project monitoring and management and the coordination of activities.

OLEMISEN will lead the Quality Management and Monitoring (QMM) activities. All partners will contribute to the evaluation process and continuous monitoring. This shall allow receiving constant feedback on the performed work and allowing partners to make corrections wherever necessary.

The WP leaders will delegate the task responsibility to consortium members, thereby engaging all partners to actively play different roles in performance of WPs.

An electronic format of this Management handbook is accessible through the MS Teams *Management > Guidelines.*

1. SCOPE MANAGEMENT

1.1. PROJECT SUMMARY

Table 1. Project information

Programme:	ERASMUS+
Call:	Partnerships for Innovation: Alliances (ERASMUS-EDU-2022-PI-ALL-INNO)
Topic:	Alliances for Education and Enterprises (ERASMUS-EDU-2022-PI-ALL-INNO-EDU-ENTERP)
Project No.:	101111732
Project name:	SMEs Cyber Security Change Agents
Project acronym:	CyberAgent
Project Duration:	01 July 2023 – 30 June 2026 (36 moths)
Type of action:	ERASMUS Lump Sum Grants
Granting authority/Agency:	European Education and Culture Executive Agency
Project coordinator:	Vilnius university

CyberAgent aims to create a platform for its target group to acquire sustainable cybersecurity and entrepreneurial knowledge and competences to inspire, empower, up-skill, re-skill and engage SME employees taking the role as Cyber Security Change Agents and involve more women in the IT sector. It will facilitate the development of collaborations between HEIs, VETs, and SMEs and operate as a platform for the sharing of best practices between players involved in cybersecurity and the labor market. Additionally, it intends to improve the employability of the target groups, support SMEs in building their cyber resilience, preserve their reputation and competitiveness, and raise organizational cybersecurity maturity and culture. The main beneficiaries affected by the Project are SME employees, in particular women, who need to be upskilled in order to play the role of a change agent in SME cybersecurity. Secondary target groups are HEIs, VETs, who will be able to implement the training content in their institutions, while HEIs students and VETs trainees will be able to use the developed content.

The up-to-date curricula and content of 8 training modules (including technical, analysis, risk management and organisational skills) for HEIs and VETs, which will be available on an online platform and may be utilized for blended learning, is part of 6 WPs that are planned.

Project results will be piloted with at least 80 participants, including at least 30 women, from 8 countries, and will be attended by 24 VET trainers and 10 HEI teachers.

Project results will be freely available to all during and after the Project end. Within 3 years after the Project's end, a training course will be offered to at least 800 more SME workers working in 100 SMEs in the partner countries. The EN versions will be used for dissemination in other European countries to expand further the localisation base.

1.2. LIST OF PARTICIPANTS

The list of the Project participants is compiled based on Grant agreement and Partnership agreement.

Table 2. List of Participants

No	Role	Short name	Project participants	Country
1	COO	VU	Vilnius university (Vilniaus universitetas)	LT
2	BEN	Moisil Buzau	Liceul Tehnologic Grigore c Moisil	RO
3	BEN	Women4Cyber	Women4Cyber Mari Kert - Saint Aubyn Foundation	BE
4	BEN	EVM	Ecosistemas Virtuales Y Modulares sl	ES
5	BEN	PRIOS	Prios Kompetanse AS	NO
6	BEN	TeknoparkMTAL	Ministry of National Education	TR
7	BEN	HACKERU	Hackeru Polska Spolka z Ograniczona Odpowiedzialnoscia	PL
8	BEN	OLEMISEN	Olemisen Balanssia RY	FI

Figure 2: Map of the Participants' Countries

1.3. LIST OF PARTICIPANTS DESCRIPTION OF THE PROJECT

CyberAgent Background

There is an average of 1.6 million cyber-attacks on a daily basis all over the world. Globally, the cost of cyber-attack losses during the year 2020 exceeded $3 trillion. A Barracuda 2022 report shows that SMEs are three times more likely to be targeted by cyber criminals than larger companies. Because of this it's important for businesses of all sizes not to overlook investment in security, both in technology and user education. The damage caused by a breach, or a compromised account can be even more costly.

The EU has become one of the regions where cyber-attacks have increased the most. The attacks mainly target technology, e-commerce, public, finance, energy and health sectors. In the "Shaping Europe's digital future" more than 70% of SMEs say they lack staff with adequate digital skills. SMEs often have fewer resources and lack security expertise, which leaves them more vulnerable to spear-phishing attacks, and cybercriminals are taking advantage.

Cybersecurity is a relatively new challenge, not integrated in the traditional educational pathways that most employees take. New skills on cybersecurity, analytical competences as well as risk management are needed, since the fight against cybercrime is complex. Not only the technical upskilling is important, as employees' attitudes, work routines and leadership should also be considered to drive change. We are talking about a "to be or not to be" in business for many SMEs.

In view of this context, Project partners decided to join their complementary forces and help SMEs to improve their cybersecurity skills and turn some of their staff as "SMEs' Cybersecurity Change Agents".

The CyberAgent project will address the following general objectives of the call:

1. Strengthen Europe's innovation by creating upskilling Ecosystems consisting of higher education, vocational education, enterprises (including SMEs) and cybersecurity stakeholders and training and enterprises (including SMEs) for introducing new skills among employees.

2. Foster multidisciplinary approaches in teaching and learning by integrating Technical, analytic and soft skills, while stimulating a sense of initiative, entrepreneurial attitudes, and developing new digital skills for workers, by developing curriculum and training modules for upskilling SME employees to the role as SMEs Cybersecurity Change Agents.

Project's general objectives

The Project aims to leverage transnational Education-Business collaboration in the cybersecurity ecosystem. It will establish a partnership among European:

1. HEIs
2. VET providers
3. SMEs

The overall aim of this partnership is for SME employees to develop competencies and become Cybersecurity Change Agents. The emphasis will be on upskilling to fill the role to deal with cyber security at normal SME workplaces.

The CyberAgent project will have the following general objectives:

4. Upgrade cybersecurity skills of European SME employees. HEIs, VET and cybersecurity training providers will design and deploy a curriculum and a training programme to increase inhouse cybersecurity competences of European SMEs. The curriculum and training programme will include modules to educate, train and follow up SMEs Cybersecurity Change Agents. After the training, the employees will achieve micro-credentials and acknowledged credits according to ECVET, EQF EQAVET, ESCO.
5. Generate exchange of good practices among cybersecurity and labour market actors. CyberAgent will develop an EU-wide digital platform to transfer knowledge to other training providers, to the general public and to keep the EU added value at its highest. The platform will support the "European Digital Innovation Hub" (EDIH) by addressing the specific needs of SMEs and public sector organisations in cybersecurity in Europe. The platform will also support the upcoming implementation of the "European Digital Education Hub" by being both a receiver of good practice as well as contributing to build the Community of Practice (CoP) part of the hub.
6. Build capacity of HEI teachers and VET providers to improve their cybersecurity competences. Our Project will produce better teachers and trainers, increase their range of academic teaching and training offerings, and find them new students and customers. HEIs teachers need to develop more relevant lifelong learning programmes and curricula to address the specific cybersecurity needs of students as future SME employees. VET providers need capacity building, train-the-trainer programmes and new tools to upskill SME employees to meet the challenges of cybersecurity.
7. Involve more women employees in cybersecurity challenges. The Project will leverage its partners' networks, especially Women4Cyber (e.g. its collaboration with ECSO on the Women4Cyber Start UP award), to boost the participation of women employees in SMEs in becoming cybersecurity change agents. CyberAgent will set minimum targets and measure women's inclusion in the training programmes. The Project will monitor the amount of women trained through the CyberAgent training programme and promote outcomes and showcase results on social media, to EU policy makers, and the cybersecurity industry.

Project's start and the budget

The Project starts on 01 July 2023 and ends on 30 June 2026.

The Project budget is of 1 494 836.00 EUR.

Main Project documents

The main Project documents are:

- the Grant agreement, signed between EC and each Project participant,
- and the Partnership agreement, signed between the Project Coordinator and partners, which is detailing and supplementary document to the Grant agreement.

The Partnership agreement is the internal contract of the Project partners which is signed and is accepted by all partners. It defines the Consortium internal rules for Project management as well as the Consortium organization. In case of discrepancy, the Partnership agreement is overruled by the Grant Agreement.

The Grant agreement includes the following annexes:

- Annex 1. Description of the action (DoA).
- Annex 2. Estimated budget (Lump Sum breakdown) for the action.
- Annex 3. Accession form for beneficiaries.
- Annex 4. Financial statement for the action for reporting period.
- Annex 5. Specific rules.

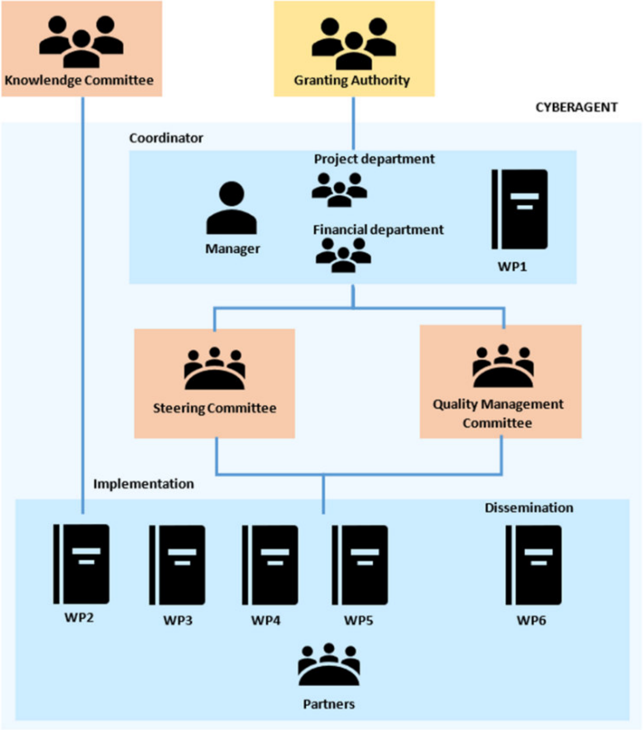
The Partnership agreement includes the following annexes:

- Annex 1. Detailed budget relating to the activities of the beneficiary.
- Annex 2. Description of the beneficiary's tasks and responsibilities.

The Grant Agreement and its annexes are available for all partners via the EU Funding & Tenders Portal (Portal). The Partnership agreement will be available for all partners in MS Teams in their private repository in *Files > Agreement*.

1.4. ORGANISATIONAL STRUCTURE OF THE CONSORTIUM

Figure 3: Organisational Structure of The Consortium



1.5. CONTACT PERSONS

The contact person of each institution appointed two or three other persons who will be willing to commit their time in creating the outcomes of the Project. During the kick-off meeting all partners provided contact persons responsible for outcomes development. There are 23 contact persons in the list. The list of contacts is available in MS Teams WP1-Management > contacts.xlsx.

The contact list must be updated when there are changes in staff or when new staff are recruited. The list of responsible persons must be reviewed at least every 6 months, either online or during face-to-face meetings.

1.6. STEERING COMMITTEE

The Steering Committee is responsible for overseeing the Project, comprising representatives from all partners' organisations. This committee plays a crucial role in the Project's execution, ensuring that it proceeds smoothly and achieves its set goals and outcomes.

Key functions of the Steering Committee include:

- Strategic Direction: The committee establishes project-defining strategies and objectives, taking into consideration the interests and needs of each organization involved.
- Risk Management: It identifies and assesses potential Project risks, as well as takes measures to mitigate and address them.
- Oversight and Reporting: The committee regularly reviews Project progress, reporting on the Project's status to the participating organizations and funders.
- Decision-Making: The Steering Committee makes significant decisions related to the Project's execution, involving representatives from all partners and seeking consensus.
- Coordination: It coordinates the collaboration of all partners, ensuring that all activities are harmonized and work synergistically.

The main activities of the Steering Committee are:

- Approval of the work plan and of the dissemination and communications plan.
- Approval of the Project's budget expenditures and allocation of the grant to partners.
- Validation of the incurred expenditure in accordance with the budget.
- Support the Coordinator in preparing meetings with the Erasmus+ Grant Authority.
- Approval of the accession of a new partner or withdrawal of an existing partner.
- Review and approve exploitation, dissemination and communication activities.

During the First online Meeting (on the 3rd of July 2023), a project Steering Committee (SC) was suggested. During the kick-off meeting in Kaunas, the SC was approved and signed by the 8 responsible representatives. The approved list with signatures is available in MS Teams *WP1-Management > Committees*.

The SC must be updated when there are changes in staff or when new staff are recruited. The list of the SC members must be reviewed at least every 6 months, either online or during face-to-face meetings.

An organisation is represented by one person and has one vote in the decision. Decisions are taken by majority vote of the SC representatives, and in all cases must be approved by either the Coordinator or the quality partner.

The SC will support the Coordinator in coordinating activities and will be responsible that all EU funding requirements and legal and ethical obligations will be met with the Project.

The Coordinator will organize a Steering Committee (SC) meeting every 6 months.

1.7. KNOWLEDGE COMMITTEE

A knowledge committee will be established in each partner country according to the CyberAgent knowledge committee guidelines.

The aims of the committees are: to facilitate further research in WP2 and support the adaptation of SME cyber security change agent qualifications. In addition, the committee will work to develop the strategy for involving more women employees in cybersecurity challenges. Members of the committees might be: Academics, HEI, VET providers, cyber security companies, organizations providing support to SMEs or dealing with cyber security one way or another etc.

Recommendations for the establishment of the Knowledge committee are provided in Guidelines for Establishing a Knowledge Committee (D.2.1 Deliverable).

1.8. STAKEHOLDERS ENGAGEMENT PLAN

The WP 6 leaders will develop a Stakeholder engagement plan that will be used to identify and track the most suitable stakeholder avenues to disseminate, elicit requirements about, and exploit the project outcomes. The engagement plan will include an outreach strategy and the organisation of 6 stakeholder workshops at M6, M10, M14, M20, M26, and M32. An initial Stakeholder Engagement Plan will be delivered in M6 and subsequent reports summarising the progress on the stakeholder engagement and workshops will be released at M12, M24, and M36. SME partners will help develop the network of SME stakeholders while Women4Cyber will provide the link to the women in cybersecurity community. Women4Cyber will help promote the project's contribution towards gender balance by engaging women in the SME Cyber Security Change Agent programme and showcasing best practices and success stories from women participants. The project will be able to benefit from ongoing actions and best practices from Women4Cyber on skills development and gender diversity in cybersecurity. All partners will focus on engaging with stakeholders and communities relevant to the project objectives:

- HEI and VET providers;
- women in cybersecurity;
- SME industry, SMEs and cybersecurity stakeholders;
- public and private agencies working in the field of cybersecurity;
- business support agencies;
- business mentors and coaches;
- research and academic communities.

1.9. PREPARATION AND ORGANISATION OF MEETINGS

The transnational meetings are planned in two main forms: face-to-face meetings and on-line partnership meetings. In all meetings, at least one representative from all partner organisations will participate. If someone is unable to join the meeting, they can find out about the meeting and the list of planned activities and issues by reading the minutes of the meeting or by contacting the Coordinator.

The Coordinator convenes online meetings at least once per month and convenes extraordinary meetings at any time upon written request of any Partner. After the decision of the partners, monthly meetings are organized every Wednesday of the first week at 10:00 CET.

The dates of online monthly meetings (over the next 7 months):

- 08-11-2023
- 06-12-2023
- 03-01-2024
- 07-02-2024
- 06-03-2024
- 03-04-2024
- 08-05-2024

This list of meeting dates is updated at the time of the physical meetings.

Face-to face meetings are organized by the planed schedule according to the application.

Table 3. Face-to-face events, meetings and mobility

Event No (continuous numbering linked to WP)	Host Partner	Description					Attendees
		Name	Type	Area	Location	Duration (days)	Total
E1.1	Vilnius university	Kick-off meeting	Partners meeting	Project Management	Kaunas, Lithuania	2	14
E2.3	Ecosistemas Virtuales y Modulares S.L.	Partners meeting for WPs management	Partners meeting	Project Management	Tenerife, Spain	2	14
E3.4	HackerU Polska	Training the Trainee LTT	Training	Skills and knowledge about cybersecurity and entrepreneurship; knowledge how to organise pilot trainings	Warsaw, Poland	3	21
E3.6	Women4Cyber	Final meeting for WPs management	Partners meeting	Project Management	Brussels, Belgium	2	14

The tasks of the first kick-off meeting in Lithuania are wider compared to all other meetings as some additional topics will be included to the Agenda, like: Project management issues, reviewing of the Risk management plan, define the Project's Steering Committee, confirm the main rules of communication and cooperation, introducing about financial rules and financial reports, detailed Gantt chart, internal quality evaluation strategy, development of the Project website and logo, dissemination plan, discuss about implementation issues.

The Coordinator gives written notice of a meeting to each Partner as soon as possible and no later than 7 calendar days preceding an ordinary meeting and 4 calendar days preceding an extraordinary meeting. The Coordinator prepares and sends each Partner an agenda. Host partner provides useful information about meeting place and accommodation. Any Partner may add an item to the original agenda by written notice to the Coordinator no later than 5 calendar days preceding the meeting and 1 day preceding an extraordinary meeting. The coordinator reserves the right to reject proposals to add to the agenda by sending an explanation.

Any decision may also be taken without a meeting. The decision will be binding after the Coordinator sends a notification to all Partners. The Coordinator will keep records of the votes and make them available to the Parties on request.

The Coordinator produces minutes of each meeting with further tasks and responsibilities for each partner, thus the Minutes will serve as a monitoring tool between the partnership meetings. It will be the formal record of all decisions taken. The Coordinator sends draft minutes to all Members within 10 calendar days of the meeting.

The minutes shall be considered as accepted if, within 5 calendar days from receipt, no Party has sent an objection to the Coordinator with respect to the accuracy of the draft minutes by written notice.

The structure of the agendas for each meeting except the first one will be as follows:

- Evaluation of the management to ensure that the Project implementation is achieved timely, and activities are fulfilled according to the Gantt chart. Responsible - VU;
- Financial management and financial reports - VU;
- Evaluation of the quality of the results related to the development of the intellectual outputs – VU and OLEMISEN.
- Discussions about further activities and tasks of the partners in producing the intellectual outputs.

Responsible partners are those who lead production of the intellectual outputs and co-lead of the specific to this output activities.

The agendas of other face-to-face meetings and online meetings will be developed according to described above structure.

1.10. QUALITY CONTROL

OLEMISEN will lead a task "Quality Management and Monitoring" of Work Package 1.

During the kick-off meeting in Kaunas the Quality Monitoring Committee (QMC) was approved and signed by the 8 responsible representatives. The approved list with signatures is available in MS Teams *WP1-Management > Committees*.

Under the leadership of Olemisen, the QMC team will evaluate quality using the following crucial criteria:

- The state of the Project;
- Partner satisfaction;
- The impact on the target groups;
- WP (Deliverables) Assurance;
- Financial Assurance.

Together with the QMC leading Olemisen the partners will closely monitor the Project's activities in relation to the accomplishment of the results and milestones in order to produce excellent results. This will be supplemented by specialized monitoring, evaluation, and reflection sessions in the Project's online and international partner meetings.

The QMC will oversee the overall progress of the Project and coordinate the execution of each task in terms of technical content and according to common quality guidelines. The QMC is the Project's Quality decision-making body in charge of issues investigation and resolution, and building a shared knowledge base leveraging the expert advice from partners. The main activities of the QMC are:

- Define the technical roadmaps for the Project.
- Approve Project baseline (schedule, effort and budget allocation, milestones and reports).
- Prepare the program of activities, and propose changes to the Project if necessary.
- Solve cross-deliverable technical issues. The QMT will facilitate mitigation and elimination of technical issues across tasks and it is composed of one representative of each partner (1 Project Manager). QMT meetings (via conference calls) will take place on a monthly basis.

All Partners will perform their part of the work according to their internal quality control and assurance procedures. If necessary, quality issues will be on the agenda of the Project meetings, possibly resulting in preventive or corrective actions. The overall quality of the execution of the research programme is also controlled using milestones and deliverables, and updated timetables within the Project. The Leaders of Project activities will regularly (at least monthly, e.g., by online meetings) inform the Project Coordinator on the detailed progress of the Project activities, on the status of milestones and deliverables, and on possible problems or delays.

From the very start of the Project, there will be an internal evaluation made by all the partners in their institutions, reported to the Project Coordinator. The evaluation will include the following points:

- Work progress in terms of partnership cooperation, communication, and Project management.
- How this progress meets the Project terms agreed upon.
- Whether this progress fits within the planned budget and time limits.
- How the work progresses regarding the dissemination plans and activities.
- How will the Project progresses in terms of sustainability and future benefits as described in the Project plan.

The means of evaluation will include active online discussion between the Project participants in addition to the formal reports on the progress. The main forum for these discussions is the monthly on-line Monitoring and steering meetings (MSM). If the MSM notice any deviations from the plans, the task of the MSM is to consider how the deviation will be corrected and authorise the right people do carry this out. The MSM will keep records on the advancement of the Project. The online meetings will produce recommendations for further development steps in the Project partner organisations.

For the Intellectual Output developments, a four-eyes-principle will be installed. Furthermore, handover templates and reports are used for a smooth progress from one activity to the subsequent one.

Indicators of the CyberAgent project are as follows in the Table 4.

Table 4. Indicators of the CyberAgent Project

Outcome	Indicators
1 partnership agreement and 1 quality management plan are in place.	Minutes of consortium meetings record progress indicated in the partnership agreement and quality management plan.
One transnational mobility programme to train SME Cybersecurity Change Agents trainers. A well described and easy to implement SME Cybersecurity Change Agent training programme in each partner country.	8 training events, 80 attendees from the target groups, with minimum 30 women, from 8 countries. Boost camp in Poland for trainers.
The curriculum will fit the ESCO skills pillar and connect to offering micro[1]credentials in European higher education. The curriculum will be divided into three themes: technical skills, analytic skills, risk management and organizational skills.	8 training modules produced, 10 HEI teachers recruited 80 students who will pilot test the curriculum from 8 countries by the end of the Project and 240 within 3 years after.
One EU-wide digital training programme	8 training toolkits produced, 24 trainers

Outcome	Indicators
delivered to train and implement SME Cybersecurity Change Agents. The programme will consist of 8 modular courses in a digital format which will be easy to adapt by each consortium partner for their own countries and contexts.	recruited, 80 SME employees from 8 countries by the end of the Project. By 3 years after Project the numbers will be 3 times as high.
8 country-specific digital learning ecosystems, one per each partner country, to engage the local SMEs community and policymakers, VETs and HEIs to exchange ideas, formats and concrete initiatives to upskill SME Cybersecurity Change Agents.	32 of target group members outreached by the ecosystems, in 8 countries by the end of the Project. 1 workshop with EU policy makers in Brussels, organised by Women4Cyber. 8 Project knowledge committee established in 8 countries. To bring expertise and professional experience within the represented sector to the evaluation of Project outputs and consultation on Project implementation and procedures. Organise a roundtable discussion with representatives of the National Digital Coalitions, presenting the results of the Project and suggesting the inclusion of training in national initiatives and national projects.
A EU-wide digital platform to improve the knowledge transfer developed among consortium partners, other training providers and the general public and to keep the EU added value at its highest.	160 of target group members registered on the platform, 48 matches made on the platform, 1200 of visits/downloads etc in 8 countries by the end of the Project. 30 women from 8 countries will have participated in at least one SME Cybersecurity Change Agent training.

The indicators of achievement and the related goals put in place are the following:

Project process (project management):

- 90% of deliverables no later than 1 month after deadline.

Partner satisfaction (collected by questionnaire at the end of every face-to-face Project Meeting):

- equal or higher than 80% of highest attainable score on a Likert-type scale (5 points).

Impact on target groups (dissemination and exploitation):

- number of members of target groups informed about the Project,
- number of members of target groups involved in the Project (i.e., participants in the pilots) no less than 80% of the goal set in the Project.

Results (quality of Intellectual Outputs):

- feedbacks about the Intellectual Outputs collected with target groups (if applicable): scores no less than 80% of the highest attainable score on a Likert-type scale (5 points).

Three dimensions will be monitored in this Project:

1. Project process: it must be assured that the Project work plan is carried out smoothly, deliverables are produced as planned and cooperation between partners is good.
2. Impact (resulting from dissemination and exploitation activities): it must be assured that target groups know and use the products and methodologies developed by the Project, and targets planned for dissemination and exploitation are met.
3. Results: it must be assured that products and methodologies developed by the Project are considered of high standard and appreciated by the target groups.

The quality of the Project activities and results will be monitored and evaluated with the following tools:

1. Internal Evaluator: Olemisen will collect information about Project managing, impact and results by accessing the internal website, the Progress Reports, the minutes of the face-to-face meetings and online meetings (MS Teams) and by examining the satisfaction questionnaires administered to the partners. Olemisen will produce the Quality Handbook, the Satisfaction Questionnaire for partners, and one Evaluation Report every 6 months
2. Quality Handbook.
3. Satisfaction Questionnaire for partners. The questionnaire will collect information about overall Project management, communication, and cooperation between partners, realized quality of products, compliance with the procedures and deadlines, etc. It will be administered at the end of every face-to-face Project meeting.
4. Satisfaction Questionnaires for target groups. Specific questionnaires about the perceived quality of every intellectual output will be administered to the members of target groups involved in the Project. Every questionnaire will be developed by the partner in charge of development of the related intellectual output.
5. Periodic Reports (to be delivered by every partner every 6 months): Every Report will contain information about (1) state of deliverables, (2) incurred costs, (3) dissemination and exploitation activities carried out, including the number of members of target groups involved (if applicable) and the quality of the intellectual outputs as realized by target groups.

6. Final Report (to be submitted by the Applicant to the EACEA): Every report will describe Project activities and results.
7. Dashboard: The Dashboard will be based on the Evaluation Reports and list the main indicators for each of the three aspects to monitor in the Project and located in MS Teams. The Dashboard will be managed and updated every six months by the persons responsible for quality assurance.
8. The Project Managers will be key staff and selected according to their experience with already managed projects and monitoring activities.
9. Dissemination: external visibility and appreciation of results.

Quantitative progress will be measured (more about indicators in the previous section):

- Multiplier events: (number, attendees, external attendees, place, and dates).
- Dissemination (in addition to research indicators): visibility Project website, social media (number of views); vision workshops and multiplier events (number of participants).
- Deliverables: timely delivery of deliverables (Project plan, milestones, deliverable name, date); evaluation of deliverables by evaluators, pilot training (number of participants, feedback).
- Management: impact (meeting participants and list of decisions, dates); interim and final report.

The detailed information about quality management is presented at The Quality Assurance and Monitoring Plan (QAMP – D1.3 Deliverable) for the CyberAgent project. It is designed to ensure the quality and effectiveness of the Project from its first step to its completion. The plan will serve as a guiding document for the Project team to maintain the quality of deliverables, monitor progress, and evaluate the Project's impact.

Gantt's chart prepared for this application will also serve as an indicator of the activities to be accomplished by certain deadlines.

Table 5. Gantt's Chart of the CyberAgent Project

Activity	2023		2024				2025				2026			
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 1.1 - Project Management	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
Task 1.2 Financial coordination	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
Task 1.3 Quality Management and Monitoring		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
Tasks 2.1 CyberAgent knowledge committees ‘establishment		▨												
Task 2.2 Mapping the training needs for SME Cyber Security Change Agents.	▨	▨												
Tasks 2.3 New professional learning pathways for upskilling of cybersecurity skills among European SMEs		▨	▨	▨										
Task 2.4 Training implementation requirement		▨	▨	▨										
Task 2.5 CyberAgent collaboration platform needs analysis		▨	▨	▨										
Task 3.1 Development of the 8 training modules at HEI level EQF6.					▨	▨	▨	▨						
Task 3.2 Development of the 8 training modules at VET level - EQF5					▨	▨	▨	▨						
Task 3.3 Designing and development of training materials					▨	▨	▨	▨						
Task 4.1 UI/UX platform prototype design and testing					▨	▨								
Task 4.2 Architecture and Structure						▨	▨							
Task 4.3 Development, testing and Quality management							▨	▨	▨	▨	▨	▨		
Task 4.4 Translation of the platform`s content in all languages										▨	▨	▨		
Tasks 4.5 Platform delivery and maintenance											▨	▨		
Task 5.1 Formalisation of local and regional network		▨	▨	▨										
Task 5.2 Train the trainer Boostcamp. 3 days training.									▨					
Task 5.3 Practical upskilling of SME Cyber Security Change Agents											▨	▨		

Activity	2023		2024				2025				2026			
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 5.4 Training Program Evaluation											■	■		
Task 6.1 Communication and dissemination		■	■	■	■	■	■	■	■	■	■	■		
Task 6.2 Stakeholder engagement		■	■	■	■	■	■	■	■	■	■	■		
Task 6.3 Policy recommendations					■	■	■	■	■	■	■	■		
Task 6.4 Good practice guide for SMEs											■	■		

1.11. BLUEPRINTS OF THE QUESTIONNAIRES

Satisfaction Questionnaires to be administered to the partners after transnational Project Meetings

- Evaluation questionnaire Kick-off meeting, Kaunas, Lithuania
- Evaluation questionnaire of 2nd transnational meeting
- Evaluation questionnaire of 3rd transnational meeting
- Evaluation questionnaire of 4th transnational meeting

Satisfaction Questionnaires for WPs

- WP1 evaluation questionnaire for partners
- WP2 evaluation questionnaire for partners
- WP3 evaluation questionnaire for partners
- WP4 evaluation questionnaire for partners
- WP5 evaluation questionnaire for partners
- WP6 evaluation questionnaire for partners

WP5 evaluation questionnaire for target groups

Satisfaction Questionnaires for Partners

- No 1 Satisfaction questionnaire for partners (1-6-month period)
- No 2 Satisfaction questionnaire for partners (7-12-month period)
- No 3 Satisfaction questionnaire for partners (13-18-month period)
- No 4 Satisfaction questionnaire for partners (19-24-month period)
- No 5 Satisfaction questionnaire for partners (25-30-month period)
- No 6 Satisfaction questionnaire for partners (31-36-month period)

WPs evaluation questionnaire for external evaluators

2. SCHEDULE MANAGEMENT

2.1. TASKS

The work of the consortium will be divided into three main phases:

1. Designing, pilot testing and delivering a tailored cybersecurity curriculum for HEI entrepreneurship students. The curriculum will address the necessary digital skills and competences to help students become Cybersecurity Change Agents in SMEs. The curriculum will be built from the existing Bachelor and Master programmes available in the partner HEIs and strengthen the current HEIs' programmes in the field of entrepreneurship and digital business. The curriculum will also increase the competence of HEI teachers on the topic of cybersecurity.
2. Designing, pilot testing and delivering a cybersecurity training programme where VET providers (trainers) will upskill SME employees (trainees). This programme will be based on an ambitious blending of offline and online training materials that will build capacity of SME employees on cybersecurity topics such as technical skills, analytic skills, risk management and organisational skills.
3. Developing a full set of digital cybersecurity services for SMEs that go beyond and complement the cybersecurity curriculum and training. The CyberAgent set of services will range from a digital platform, an interactive tool that will allow for dissemination of the most prominent cases of training Cybersecurity Change Agents in SMEs, to the organisation of international bootcamps, offering SME employees dedicated learning activities on cybersecurity and the possibility to exchange experiences with their peers at EU level.

In addition to these specific phases, the CyberAgent will also implement transversal activities, such as management and quality assurance, evaluation of the knowledge programmes and services offered by the Project and dissemination and exploitation actions.

The overall plan of the Project follows the tasks and activities and schedule as laid down in the Work Plan (Annex 1 to the grant agreement AND Annex 2 to the Partnership Agreement).

The Project is organised in the following Work Packages:

Table 6. Work Packages of the CyberAgent Project

Work package No	Work Package name	Lead beneficiary	Effort (Person-months)	Start month	End month
WP1	Project management	VU	81.91	1	36
WP2	CyberAgent approach and structure design	OLEMISEN	60.95	4	12
WP3	CyberAgent Learning resource development	TeknoparkMTAL	50.56	3	24
WP4	CyberAgent Collaboration Digital Platform	VU	59.05	1	36
WP5	Boost CyberAgent Upskilling at local and regional level	EVM	53.99	3	35
WP6	Dissemination & Exploitation	Women4Cyber	55.24	1	36

Each Work Package has a Leader who is responsible for the preparation of any technical reports, achieving milestones, deliverables and provision of deliverables, periodic reports to the Coordinator on schedule. The partners concerned shall appoint named individuals to carry out the Work Package fulfilling "The staff cost of the management and implementation staff of the project" and "The role and functions of the management and implementation staff of the project" forms.

Work packages and their activities with expected results are presented in the table below.

Table 7. Work Packages and Their Activities with Expected Results

Work package	Activity title	Estimated start date	Estimated end date	Expected results
WP 1 - Project management	Management handbook	01.07.2023 (4 months)	31.10.2023	The report, which will be written in English, will provide information on how to manage the Project effectively. The document will be in PDF format, 20 pages.
	Project Face-to-Face meetings reports	01.07.2023 (30 months)	31.12.2025	The report, which will be produced in English, will include a description of the meeting, the agenda, the presentations, the list of participants, photos of the meetings, the meeting report, together with an evaluation of participants' satisfaction. The report consists ~30 pages. The document will be in PDF format.
	Quality Assurance and Monitoring Plan	01.07.2023 (4 months)	31.10.2023	The report, which will be written in English, will include guidelines and indicators for Project monitoring and quality assurance. The document will be in PDF format, 20 pages.
	6 reports for each WP	01.07.2023 (36 months)	30.06.2026	The reports, which will be written in English, will indicate the progress and results of the Project tasks. An annual report will be produced and updated during the Project. The document will be in PDF format.
	Financial report	01.07.2023 (36 months)	30.06.2026	The report, which will be produced in English, will show the budget, the budget spent by product and the plan, both for the Project as a whole and for each partner. An annual report will be produced and updated throughout the Project. The document will be in PDF format.
WP 2 - CyberAgent approach and structure design	CyberAgent knowledge committee guidelines	01.07.2023 (4 months)	31.10.2023	Recommendation for tasks and how committee will work and collaborate. Electronic format/pdf max 20 pages in English.
	The SME Cyber Security Change	01.07.2023 (10 months)	30.04.2024	Comprehensive report of the need analysis. Electronic format/pdf

Work package	Activity title	Estimated start date	Estimated end date	Expected results
	Agents Training needs mapping report			document in all partner languages.
	SME Cyber Security Change Agents learning pathway's structure	01.07.2023 (12 months)	30.06.2024	Comprehensive reports: A. The content outline (objective, learning outcomes in terms of knowledge/skills/competences, duration, content, training methods and assessment types, EQF level, ECTS etc.) of the 8 training schemes proposed The curriculum for VET level. The curriculum for HE students The curriculums includes implementations of Microcredentials B. The training methodology C. The assessment methodology. Electronic format/pdf and ePub document in all partner languages.
	The SME Cyber Security Change Agents Training implementation requirement plan	01.07.2023 (12 months)	30.06.2024	A complete implementation plan covering the findings from D2.1 – D2.3. Max 20 pages. Electronic format/pdf and ePub document in all partner languages.
	CyberAgent collaboration platform requirements report	01.07.2023 (12 months)	30.06.2024	Requirement report of end users' expectations for platform and functionality demands. Electronic format/pdf 10 pages in English.
WP 3 - CyberAgent Learning resource development	Training modules for HEI students	01.07.2023 (24 months)	30.06.2025	8 syllabuses for training modules. Electronic format/pdf in English and partner languages.
	Training modules for VET students	01.07.2023 (24 months)	30.06.2025	8 syllabuses for training modules. Electronic format/pdf in English and partner languages.
	Training Materials Documents and Videos	01.072023 (24 months)	30.06.2025	The suite of training material will include: a) The training material for HE b) The training material for VET c) The training material for SME Cyber Security Change Agent

Work package	Activity title	Estimated start date	Estimated end date	Expected results
				training. The material will be comprised of a mixture of traditional content as well as cutting- edge learning resources. The core material will be developed in all languages of the consortium. Any videos will be developed in English with subtitled and/or voice over. Electronic Format (PDF, PPT, video). All partner languages.
WP 4 - CyberAgent Collaboration Digital Platform	Peer-reviewed and finalized UI/UX prototype	01.072023 (24 months)	30.06.2025	Online link to a prototype in English.
	Operational platform	01.07.2023 (30 months)	31.12.2025	Online link to a pilot version of the platform, in English and all partner languages.
	Platform fine-tuned and translated	01.07.2023 (36 months)	30.06.2026	Online link to a final version of the platform, in English and all partner languages.
WP 5 - Boost CyberAgent Upskilling at local and regional level	Documented local and regional CyberAgent upskilling network	01.07.2023 (12 months)	30.06.2024	Description of Network. PDF in English. Maximum 16 pages.
	Boost camp in Poland for trainers.	01.07.2023 (26 months)	31.08.2025	Train the trainer program with evaluation. The train the trainer program available in English. PDF maximum 30 pages.
	CyberAgent upskilling Training Program Evaluation	01.07.2023 (34 months)	30.04.2026	Evaluation report after piloting. Electronic format/pdf 20 pages in English.
	Teaching methodology for SMEs Cyber Security Change Agents	01.07.2023 (35 months)	31.05.2026	Online toolkit in English and the partner languages for at Collaboration platform.

Work package	Activity title	Estimated start date	Estimated end date	Expected results
WP 6 - Dissemination & Exploitation	Dissemination & communication strategy (incl. Progress reports at M12, M24, and M36)	01.07.2023 (3 months)	30.09.2023	Dissemination & communication strategy. The documents will be written in English, format: PDF. Max 20 pages.
	Stakeholder engagement plan (incl. Progress reports at M12, M24, and M36)	01.07.2023 (6 months)	31.12.2023	Progress reports, which will be produced in English, will include a description of the stakeholder workshops, the agenda, the presentations, the list of participants, photos of the meetings, the meeting report, etc. Format: PDF. Max 15 pages.
	Policy recommendations	01.07.2023 (36 months)	30.06.2026	The documents will be written in English, format: PDF. Max 20 pages.
	Good Practice Guide for SMEs	01.07.2023 (36 months)	30.06.2026	The documents will be written in English and localized to partner languages, format: PDF. Max 20 pages.
	Final Conference	01.07.2023 (36 months)	30.06.2026	An international conference in English for 50 participants.

2.2. DELIVERABLES

Each WP will have deliverables associated with it. It is important throughout the Project that all deliverables are rigorously tracked and implemented and achieved on time.

If one or more of the Partners is late in submission of any Project deliverable, the Coordinator may nevertheless submit the other Parties' Project deliverables and all other documents required by the Grant Agreement to the Granting Authority in time.

The list of deliverables for the 36 months of the Project is shown in chronological order below.

Table 8. Deliverables

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D6.1	Dissemination & communication strategy (incl. Progress reports at M12, M24, and M36)	WP6	3 - Women4Cyber	R — Document, report	PU - Public	4

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Management handbook	WP1	1 - VU	R — Document, report	PU - Public	4
D1.3	Quality Assurance and Monitoring Plan	WP1	8 - OLEMISEN	R — Document, report	PU - Public	4
D2.1	CyberAgent knowledge committee guidelines	WP2	8 - OLEMISEN	R — Document, report	SEN - Sensitive	4
D6.2	Stakeholder engagement plan (incl. Progress reports at M12, M24, and M36)	WP6	3 - Women4Cyber	R — Document, report	SEN - Sensitive	6
D2.2	The SME Cyber Security Change Agents Training needs mapping report.	WP2	8 - OLEMISEN	R — Document, report	PU - Public	10
D2.3	SME Cyber Security Change Agents learning pathway's structure	WP2	1 - VU	R — Document, report	PU - Public	12
D2.4	The SME Cyber Security Change Agents Training implementation requirement plan	WP2	8 - OLEMISEN	R — Document, report	SEN - Sensitive	12
D2.5	CyberAgent collaboration platform requirements report	WP2	5 - PRIOS	R — Document, report	PU - Public	12
D5.1	Documented local and regional CyberAgent upskilling network	WP5	4 - EVM	R — Document, report	SEN - Sensitive	12
D4.1	Peer-reviewed and finalized UI/UX prototype	WP4	5 - PRIOS	OTHER	PU - Public	16
D3.1	Training modules for HEI students	WP3	1 - VU	OTHER	PU - Public	24
D3.2	Training modules for VET students	WP3	6 - TeknoparkMTAL	OTHER	PU - Public	24
D3.3	Training Materials Documents and Videos	WP3	7 - HACKERU	OTHER	SEN - Sensitive	24
D5.2	Boost camp in Poland for trainers.	WP5	7 - HACKERU	R — Document, report	PU - Public	26
D1.2	Project Face-to-Face meetings reports	WP1	1 - VU	R — Document, report	PU - Public	30
D4.2	Operational platform	WP4	5 - PRIOS	OTHER	PU - Public	30

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D5.3	CyberAgent upskilling Training Program Evaluation	WP5	8 - OLEMISEN	R — Document, report	PU - Public	34
D5.4	Teaching methodology for SMEs Cyber Security Change Agents	WP5	4 - EVM	OTHER	PU - Public	35
D1.4	6 reports for each WP	WP1	8 - OLEMISEN	R — Document, report	SEN - Sensitive	36
D1.5	Financial report	WP1	1 - VU	R — Document, report	SEN - Sensitive	36
D4.3	Platform fine-tuned and translated	WP4	5 - PRIOS	OTHER	PU - Public	36
D6.3	Policy recommendations	WP6	3 - Women4Cyber	R — Document, report	PU - Public	36
D6.4	Good Practice Guide for SMEs	WP6	1 - VU	R — Document, report	PU - Public	36
D6.5	Final Conference	WP6	3 - Women4Cyber	OTHER	PU - Public	36

Partners responsible for these deliverables must be cautious with the submission of these deliverables. All the deliverables must be finalised and submitted within the deadlines defined in Annex I to the Grant Agreement. The WP leaders are responsible for the technical quality of the deliverables.

The delivery number shall be used as a code of all deliverables. The title of the document/deliverable must follow the titles included in the work programme.

3. FINANCIAL MANAGEMENT

The financial management of the Project will deal with the budget, control, accounting and reporting actions.

In September of 2023, a Partnership agreement was signed between the Coordinator and the other partners clarifying each other's responsibilities, tasks and the respective financial contributions from the Project grant. The Project budget will be managed by the Coordinator and the grant is allocated according to the terms and conditions set out in the Erasmus+ Grant Agreement and the Partnership agreement. The budget detailed per partners and the corresponding EU contribution of each partner is detailed in the Annex 2 of Grant agreement and in the Annex 1 in Partnership agreement. The EC contribution of each of the partners is a maximum contribution conditioned to the acceptance by the EC of expenses up to the budget of the partner. If a partner spends less than what it is shown in its approved budget (or the Commission does not accept all its costs), it will receive only the proportional part of the EC contribution).

The almost uniform distribution of planned activities among partners in the consortium is reflected in the budget distribution. The Partnership agreement foresees the contractual obligations, including a commitment to spend the available resources in a coherent and economical way. The Partnership agreement states the financial commitments for each partner and the related reporting/payment schedule.

At the online kick-off meeting (month 1) the partners were introduced to the financial and administrative rules in detail and provided with forms for reporting. Periodic financial reports of each partner will ensure control over the money spent. Personal consultations with the Coordinator's financial officer will take place at the end of every consortium meeting, if necessary. Reference and update on the financial and administrative rules will also be provided during each consortium meeting.

The Project Coordinator together with the finance officer will inform partners about finance management by using online tools, and will consult them online, if partners have financial questions. The detailed presentation about finance management was presented during face-to-face kick-off meeting in Kaunas, and templates provided for registering the costs of activities carried out by the partner.

The Coordinator will also lead the financial management of the Project, ensuring that the effort of each partner will not deviate from the plan and will follow the path designed during the proposal preparation.

The main tool for the financial management will be the creation and delivery of a total amount of 6 financial and management reports templates which will be filled in by all partners. These reports will be produced on a 6-months basis and will give a comprehensive picture of the project's financial situation for the period taken into account. After the first cycle of the intensive programmes, the Coordinator will ask all partners' finance officers to start sending filled with templates. Reallocation of the Project finance will be allowed only after the Coordinator approves this action (respectively, the Coordinator will consult the Grant Authority if any questions concerning financial management arise).

All the documents justifying the expenses will have to be stored by the institutions bearing the costs. The Coordinator will ask for scanned copies of these documents. For smooth finance management Coordinator will ask Partners to upload scanned financial documents to online drive (MS Teams private repository), the Coordinator will monitor the progress of the content development and react if some major delays are detected. The Project Partners will commit to produce the following key outcomes by the respective deadlines.

All the Partners will have to provide information to the Coordinator at the request, in particular for the reporting purposes.

An in-depth presentation and discussion of all financial and administrative arrangements were held in one dedicated workshop during the kick-off meeting in Kaunas.

Partners received a first payment after Partners sign Partnership agreement, but all further payments will be linked to satisfactory financial reports and eligibility of costs incurred. Only partners who have provided full documentation and justification of all previous expenditure will receive the next payment instalment.

The financial contribution of the Granting Authority to the Project will be distributed by the Coordinator according to:

- the Project Plan.
- the approval of reports by the Granting Authority, and
- the provisions of payment by the Partnership Agreement.

Table 9. Reporting and Payments

Reporting			
Reporting deadlines		Type	Payments
No	Till date		
1.	-	Prefinancing	20%, 30 days from entry into force of this Contract
2.	15-04-2024	Periodic report	20%, 30 days from receiving periodic report
3.	15-01-2025	Periodic report	20%, after Beneficiary's report approval by the Coordinator and within 30 calendar days after receiving payment from the Granting Authority after report approval
4.	15-10-2025	Periodic report	20%, 30 days from receiving periodic report
5.	15-07-2026	Final report	20%, after Beneficiary's report approval by the Coordinator and within 30 calendar days after receiving payment from the Granting Authority after report approval

Beneficiaries will be funded only for its tasks carried out in accordance with the Grant agreement and Partnership agreement.

The Coordinator will notify the Partners concerned promptly of the date and composition of the amount transferred to its bank account, giving the relevant references.

3.1. REPORTING

The Partners will carry out a self-assessment and reflect on the quality of the implementation of their Project (including a comparison between the indicators proposed at application stage and the result achieved), the successes, the problems encountered and the lessons learnt.

There are two types of reporting in the Grant Management Services in the Portal:

- Continuous reporting: available from the beginning of a project (collaborative: all beneficiaries can edit).
- Periodic reporting: available at the end of a reporting period.

PERIODIC REPORTING

In order to receive payments, the consortium must submit Periodic and Final reports according to the schedule established in the Grant Agreement.

The partners deliver reports for the Coordinator in 4 reporting periods:

- 1st reporting period: from 1 to 9 months (deadline15.04.2024).
- 2nd reporting period: from 10 to 18 months (deadline 15.01.2025). Periodic reporting.
- 3rd reporting period: from 19 to 27 months (deadline 15.10.2025).
- 4th reporting period: from 28 to 36 months (deadline 15.07.2026). Final report.

The submission of the periodic and final reports to the EC is the responsibility of the Coordinator. The Coordinator will use the electronic exchange system.

At the end of each reporting period, each beneficiary will receive a notification to complete:

- Their contribution to the Technical Part (this is common for all beneficiaries in the Project).
- Their contribution to the Status of Work Packages (this is common for all beneficiaries in the Project).

Report submission process (Lump Sum):

- Step 1: All beneficiaries receive a notification and log on to the Portal. Also, the Coordinator sends to Partners, a reminder about a Period report or the Final report submission.
- Step 2: All beneficiaries complete their contribution to the Technical Part of the Periodic Report and Lock to Review their Technical Part once completed.
- Step 3: The Coordinator completes the Status of Work Packages and Locks & Includes them.
- Step 4: The Coordinator receives a notification that the Financial Statement for all beneficiaries is ready to be signed.
- Step 5: The Coordinator reviews the elements of the Periodic Report & submits to the EU.

- Step 6: The EU reviews the submitted Periodic Report and accepts, requests additional information or rejects it.
- Step 7: Interim Payment.

The reporting process for Lump Sum grants is described in the Funding & Tenders Portal IT How To section on Lump Sum Reporting. It will be using the standard technical periodic report template available directly in the Grant Management System.

The periodic report consists of two parts, the Technical Report and Financial Report.
The Technical Report is itself also divided in two parts, Parts A and B:

- Part A: contains the structured tables with Project information (retrieved from the Grant Management System).
- Part B (the narrative part): mirrors the application form and requires the participants to report on differences (delays, work not implemented, new subcontracts, budget overruns etc.) It must be uploaded as PDF document.

The Financial Report consists of the structured individual and consolidated Financial Statements (retrieved from the Grant Management System).

The periodic reports follow the structure of the application form, with the award criteria, re-assessed by the (internal or external) experts when the Project reaches its mid-term and at its completion. The overall structure of the report is:

- Project management (report on aspects, related to the cooperation among partners, working arrangements, distribution of tasks and coordination, respect of Project timeline).
- Project implementation (report on the achievement of the objectives measured by the quantitative and qualitative indicators).
- Impact and sharing results (report on the results of the Projects were made available and produced benefits for the organisations participating in the Project and to other stakeholders. Also, the sustainability and the longer-term impact of the Project.)

The description of results will include the reference to relevant supporting documents such as meeting minutes, course materials, Project deliverables, publications, photos etc.

At the end of the Project one Final report and all necessary documents providing evidence of the achievement of reported results will be submitted. The content of the Final report is compulsory and determined by the EC.

CONTINUOUS REPORTING

During the Project, will be provided regular updates (continuous reporting) on the status of the Project in the Portal.

The continuous reporting includes:

- progress in achieving milestones

- deliverables
- updates to the publishable summary
- response to critical risks, publications, communications activities, IPRs
- programme-specific monitoring information (if required).

Tasks of the Coordinator in the reporting process:

- Checks that the Continuous Reporting Module is updated in time (before the Periodic Report is Locked for review).
- Checks that all participants have submitted their Financial Statements (and Certificate on the Financial Statements, if needed).
- Quality checks.

Table 10. Reporting summary

No	Type of report	Due Date	Responsible
1.	Periodic	15-04-2024 15-01-2025(Periodic) 15-10-2025 15-07-2026 (Final)	All partners
2.	Financial reports	31-12-2023 30-06-2024 31-12-2024 30-06-2025 31-12-2025 30-06-2026 (M36)	VU
3.	Face-to-Face Meetings reports (D1.2 deliverable))	Meeting dates (M30) 03-04.10.2023 06.2024	VU
4.	WP reports (6 reports) (D1.4 deliverable). Authorized QAMP progress reports: (1) monthly; (2) quarterly; and (3) semi annually.	M12 M24 M36	Olemisen
5.	Market Analysis Country Reports		All partners
6.	Dissemination & communication report (D6.1 deliverable)	(M12, M24, and M36)	Women4Cyber All Partners
7.	The SME Cyber Security Change Agents Training needs mapping report (D2.2 deliverable)	30-04-2024(M10)	Olemisen

No	Type of report	Due Date	Responsible
8.	SME Cyber Security Change Agents learning pathway's structure comprehensive reports	M12	VU
9.	CyberAgent collaboration platform requirements report (D2.5 deliverable)	M12	Prios
10.	CyberAgent upskilling Training Program Evaluation report	M24	Olemisen
11.	Reports summarising the progress on the stakeholder engagement and workshops (D 6.2 deliverable)	M12, M24, and M36	Women4Cyber

The coordinator will draft a template for the reports, so that all of them comply with the same structure. The reports will firstly be assessed by the task leader and then approved by the WP leader. Periodic reporting will include management (progress, conflict handling, etc.), financial and other relevant issues produced by WP leaders, who will draft the minutes of their meetings, and contribute to periodic reports, as appropriate.

4. COMMUNICATIONS MANAGEMENT

Communication management is a critical component of successful Project implementation and outcomes. Communication serves several important purposes: Project coordination, information sharing, stakeholder engagement, transparency, compliance and reporting, dissemination of results, problem-solving, networking and collaboration, public relations, risk and crisis management, innovation and technology transfer, monitoring, quality assurance and many other purposes.

Internal communication. Internally, in the Project consortium communication will consist of face-to-face and on-line meetings (personal, working groups, consortium, committees), phone calls, e-mail correspondence, handbooks and guidelines. The consortium will use an online Project management workspace MS Teams to share experiences, documents, discussions, etc. The online platform will ensure quick and easy communication between consortium members.

The communication management procedures have to guarantee that the documents in the Project are produced, updated, distributed and stored correctly and efficiently. Administrative information must be submitted directly from each Partner to the Project Coordinator.

After the Grant Agreement has been signed the Project Coordinator and the Partners informed the management / administration of their organization and appointed a person who will assist in administrative issues, a specialist of public procurement who will initiate the tender(s) for the services or/and goods to be acquired in the Project and a specialist in law who will help the Coordinator to prepare the documents for contract signing between all the partners. The tasks and roles of the partners were distributed in written to the Partners for their consideration and subsequent discussion during the kick-off meeting if necessary.

The contact person of each institution appointed one or two other persons who will be willing to commit their time in creating the outcomes of the Project. These preparatory works will ensure the efficiency of the kick-off meeting and undermine conflict possibilities in the future.

Communication will be put in place through online conference tools (MS Teams was approved as official communication platform and files repository), phone and exchange of e-mails but also via distance collaboration tools and services (MS OneDrive, Facebook and etc.). In order to ensure communication transparency, the coordinator has set up a contact / conference group that includes representatives of all partners (one email address). This list can be updated if necessary, but the partner must contact the coordinator to indicate the changes.

Additional online meetings (if necessary) are planned using Doodle which simplifies the process of scheduling.

It is particularly important that all the partners are kept informed on the Project's developments and can always contribute with their suggestions. During all the on-line meetings, the arguments will be recorded, and the minutes of the meeting will be drafted both for the creation of a participatory collaborative spirit but also for monitoring and reporting purposes.

Over the lifetime of the Project, it will be used a collaborative approach. The Project Partners will exchange good practices, reinforce their networks, increase their capacity to operate at the transnational level, share and confront ideas, practices, and methods. They will also respect co-creativity principles, encouraging transparency and guaranteeing that all participants will have equal access to the decision-making process.

External communication. External communication is needed for information and results sharing for stakeholders, stakeholder engagement, feedback and evaluation.

For external communication will be used Project website, collaborative platform for skills development, email, social media, newsletters, press release, final conference, partners network, meetings and visits to key stakeholders.

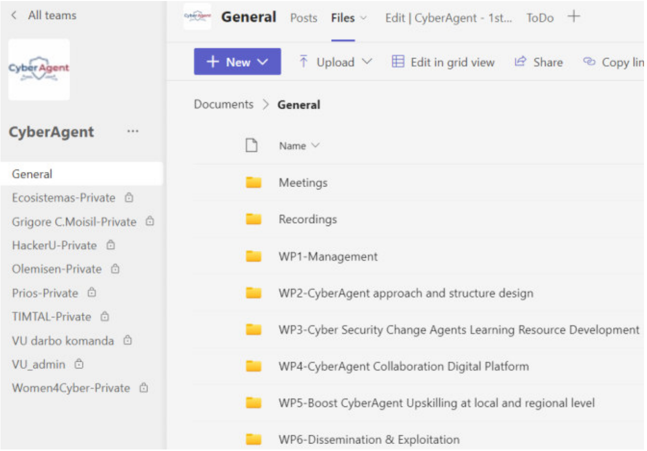
To facilitate the exchange of emails, was created a common e-mail address (contact@cyberagents.eu) of the Project for external communication.

4.1. COMMUNICATION PLATFORM

The official documentation repository for the CyberAgent project is accessible through MS Teams. MS Teams is the Project workspace for real-time collaboration and communication, meetings, file and app sharing.

MS teams has private and public repositories. The private repositories dedicated to store private documents during the Project and may be managed for the Coordinator and certain Partner. Documents in public repository can be managed by the Coordinator and all partners. A brief summary of the documentation organisation and content is given below.

Figure 4: Screenshot of MS Teams Folder Structure



CyberAgent

General
Ecosistemas-Private
Grigore C.Moisil-Private
HackerU-Private
Olemisen-Private
Prios-Private
TIMTAL-Private
VU darbo komanda
VU_admin
Women4Cyber-Private

Meetings
Recordings
WP1-Management
WP2-CyberAgent approach and structure design
WP3-Cyber Security Change Agents Learning Resource Development
WP4-CyberAgent Collaboration Digital Platform
WP5-Boost CyberAgent Upskilling at local and regional level
WP6-Dissemination & Exploitation

General repository > Files:

- Meetings
  - Online meetings
  - Face-to-face meetings
- Recordings
- WP1-Management
  - Templates
  - Guidelines
- WP2-CyberAgent approach and structure design
- WP3-Cyber Security Change Agents Learning Resource Development
- WP4-CyberAgent Collaboration Digital Platform
- WP5-Boost CyberAgent Upskilling at local and regional level
- WP6-Dissemination & Exploitation
  - Templates
  - Info about the partners
  - CyberAgent logo

General repository > ToDo (a list of the tasks and deliverables). The TODO list is important in ensuring timely completion and monitoring of the tasks.

4.2. DISSEMINATION

As Dissemination WP 6 leader, Women4Cyber will coordinate the dissemination activities and will measure their impact across the consortium partners' channels. The WP leader has proven expertise in communication plans addressing business creation, support to SME staff, entrepreneurship students and career centres. Moreover, its position as dissemination leader in the Project will ensure that the design and production of an effective dissemination strategy will promote the EU added value of the Project.

There are these target groups that should be at the receiving end of the dissemination activities undertaken on the Project: Project partners, associated partners, affiliated entities members, other stakeholders in consortium countries, research and academic communities, business associations, VET communities, IT professionals and women's associations, policy makers, regulators and public bodies like EC. National decision makers, ministry representatives, national and regional funding agencies and international institutions, civil society at regional, national and European level like students, HEI and VET teachers, unemployed people, NEETs, women, citizen, consumer, NGOs organisations and specialised media, SME employees and especially women employees.

Women4Cyber developed Dissemination & communication strategy (D6.1 Deliverable) at the start of the Project with progress reports at yearly intervals after that (incl. Progress reports at M12, M24, and M36). The strategy provides main activities, dissemination responsibilities and dissemination plan.

Each partner will be responsible for dissemination activities within their own country and using their own networks, contacts and dissemination channels. Each Partner will be responsible for planning their own dissemination activities and reporting back to the WP leader, which will design a dissemination plan template to be used for both planning and reporting purposes.

All the official documents of the Project (presentations, deliverables, communication, etc.) must use the templates which will be available in the MS Teams.

Any communication or dissemination activity related to the action must use factually accurate information. Moreover, it must indicate the following disclaimer (translated into local languages where appropriate) (see Grant agreement section 17.3) and European flag and funding statement (see Grant agreement section 17.2):

"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 [name of the granting authority]. Neither the European Union nor the Granting Authority can be held responsible for them."

For external communication and dissemination, the EU logo and a disclaimer must also be included in all the documents related to the Project. The templates may be modified during the Project duration, so it is recommended to download the templates from the Teams each time an official CyberAgent document is going to be prepared.

The detailed information about the dissemination is explained at The Dissemination & communication strategy (D6.1 Deliverable, available in MS Teams *WP6-Dissemination & Exploitation*) for the CyberAgent project.

5. RISK MANAGEMENT

The main potential problem for the Project is the case that Partners fail to live up to contractual obligations, in particular deliverables due as described in the Grant agreement. Such problems will be dealt with all Partners, when identified. Mitigation measures are provided to avoid or mitigate risks. The list of risks and mitigation measures will be reviewed and updated as necessary during partner meetings at least every 6 months.

The Project coordinator and partners are responsible for risk management processors throughout the Project, communicating these risks and cooperating in managing them. A risk register in the Portal will help implement and monitor the risk assessment strategy.

Table 11. Risk Assessment Strategy

Risk No	Description	WP No	Proposed Mitigation Measures
1.	Communication break-down between partners	WP6, WP4, WP5, WP1, WP2, WP3	Partners have had previous successful collaborations. Efficient communication will help to mitigate this risk. Partners have worked well together during the proposal stage.
2.	Change in key staff during Project	WP6, WP4, WP5, WP1, WP2, WP3	More than one person in each partner organisation is informed of the specific tasks and can be replaced as needed.
3.	Delay in a specific deliverable	WP6, WP4, WP5, WP1, WP2, WP3	Elaborate a draft report at least two weeks before the deadline and follow up with all deliverables. Clear Project management structure, division of tasks, regular meetings and calls to track progress.
4.	Partner withdrawal and/or modification of Project objectives/milestones	WP6, WP4, WP5, WP1, WP2, WP3	All partners could do the work of another partner jumping out of the Project. Prior to the Project start, partners will prepare a list of backup key personnel ready to jump in. Tasks can be reassigned to other internal/external partners as partners' networks are extensive.
5.	Insufficient interest of target groups in the digital platform and the cybersecurity training programme	WP5	Tools and resources will be developed based on the stakeholder needs identified in the needs analysis of this proposal. User feedback is collected via impact assessment after each pilot training event and users' feedback, strategy, tools and resources are adjusted/improved accordingly.
6.	Low level of impact and sustainability	WP6, WP4, WP5, WP1, WP2, WP3	Impact and sustainability are built into the work plan. The activities gradually evolve, engaging a wide range of stakeholders, collecting their needs and feedback, evaluating the impacts and adjusting the Project outputs feeding into the exploitation plan.
7.	Insufficient numbers of SME employees	WP5	The most visible SME employees will be invited to the training events to promote their learnings on

Risk No	Description	WP No	Proposed Mitigation Measures
	participate to the cybersecurity training events and/or fail to provide information on key success factors		cybersecurity as well as be given the opportunity to promote themselves in the Project's marketing channels and cross-sector publications.
8.	Last-minute cancellation of experts during bootcamp events	WP3	When planning an event, we always take into account any possible last-minute cancellations and have a list of back up speakers and moderators. Other solutions include using experienced staff of any of the partners, to step in as session leaders whenever appropriate.
9.	Technical issues with the digital platform	WP4	In the event of any issues with the platform, the IT provider of the WP leader Prios will be immediately notified and will address the problems, with the aim of having 50% of the issue solved within the first 24 hours.
10.	Assuring data security	WP4	The consortium will establish a central Project database where all relevant documents will be collected and categorised so that they can be easily found and shared. Encrypted storage for sensitive information will be created. Particular care will be taken with the handling of contact details of stakeholders, officials and others, and contact info will not be provided to outside sources without permission.
11.	Late hiring or appointing staff for the Project. Lack of human resources	WP6, WP4, WP5, WP1, WP2, WP3	The lead partner for the specific activity will ensure adequate human resources; Reallocation of tasks within the activity
12.	Representative of Project partner miss the partners management meeting	WP6, WP4, WP5, WP1, WP2, WP3	During or after the meeting, the Coordinator arranges a gathering of the MS Teams with him or her. The MS Teams platform is where the minutes of online meetings are kept. The tape can be reviewed or viewed by the person who was unable to attend the meeting. This person can get in touch with the Coordinator if they have any questions.
13.	Conflicts between partners	WP6, WP4, WP5, WP1, WP2, WP3	During the kick-off meeting, the partners will discuss in detail the responsibilities, duties and roles and agree on an equitable distribution of responsibilities to avoid such risks. The meeting report will be used as a guiding principle for all other meetings between consortium partners to reach compromise and promote cooperation. The consortium may consider reallocation of roles and responsibilities if one of the partners consistently performs poor quality work, despite repeated requests for better performance
14.	Conflicts because of intellectual property and copyright Improper use of the Project budget may	WP6, WP4, WP5, WP1, WP2, WP3	One intellectual property rights agreement will be signed to prevent potential conflicts to surface. At the beginning of the Project, certain financial cost

Risk No	Description	WP No	Proposed Mitigation Measures
	raise financial risks to the Project budget		guidelines will be established. The partners will be informed of the acceptable costs and any unacceptable costs will have to be borne by the partner institutions at their own expense.
15.	Postponement of meetings of international partners due to pandemic circumstances, e.g. COVID-19	WP6, WP4, WP5, WP1, WP2, WP3	Inform EACEA by email about the postponement. EACEA have to approve this. To organize online meetings if there are no possibilities to organize face-to-face meetings.
16.	SMEs don't see need for having internal cyber security competence	WP5	Support them with information, tailored at their business sector, which gives better idea for why needed.

BIBLIOGRAPHY AND USEFUL LINKS

1. European Commission. Erasmus+ Programme Guide. https://erasmus-plus.ec.europa.eu/erasmus-programme-guide.
2. European Commission. Visual Identity - Programming period 2021-2027. European flag emblem and multilingual disclaimer. https://www.eacea.ec.europa.eu/about-eacea/visual-identity/visual-identity-programming-period-2021-2027/european-flag-emblem-and-multilingual-disclaimer_en
3. Publication Office of the European Union. How to communicate your project. https://op.europa.eu/en/publication-detail/-/publication/429c34ff-7231-11ec-9136-01aa75ed71a1/language-en
4. KA2 Lump Sum Handbook. https://wikis.ec.europa.eu/display/NAITDOC/KA2+Lump+Sum+Handbook?preview=/75759701/75759705/Handbook%20on%20KA2%20lump%20sum%202023%20for%20publication%20final.pdf
5. European Commission. Funding & tender opportunities. Reporting process — Lump sum. https://webgate.ec.europa.eu/funding-tenders-o
6. pportunities/pages/viewpage.action?pageId=8913115
7. EUROPEANA. European Guide to Organising Online Events. https://pro.europeana.eu/files/Europeana_Professional/Event_documentation/Webinars/Europeana-Guide-to-Organise-Online-Events.pdf
8. How to manage your lump sum grants. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-manage-your-lump-sum-grants_en.pdf
9. European Commission. Additional resources. https://webgate.ec.europa.eu/erasmus-esc/home/resources/additional-resources
10. European Commission. Reports & payment requests. https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=1867970
11. European Commission. Reporting process — general. https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=8913035
12. European Commission. Funding & tender opportunities. Reference Documents (Reporting templates). https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/reference-documents?selectedProgrammePeriod=2021-2027&selectedProgramme=ERASMUS2027
13. European Commission. Funding & tender opportunities. Projects & Results. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-results
14. European Commission. Funding & tender opportunities. Reporting process — Lump sum. https://webgate.ec.europa.eu/funding-tenders-opportunities/pages/viewpage.action?pageId=8913115

CyberAgent

Co-funded by
the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas · 1579 · Universitas Vilnensis | Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LISESI

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION

Liceul Tehnologic Grigore C. Moisil BUZAU