wem cyber

D4.1

Dissemination and Communication and Exploitation Plan

Contact

coo.wemcyber@bilisimvadisi.com.tr

Funded by
the European Union

D4.1

Dissemination and Communication and Exploitation Plan

WEM Cyber
Widening Excellence and Mentoring In Cybersecurity

CALL: HORIZON-WIDERA-2024-TALENTS-03
TYPE OF ACTION: HORIZON-CSA
STARTING DATE: 1 JANUARY 2026
DURATION: 36 MONTHS
COORDINATOR: BILISIM VADISI TEKNOPARK YONETICI AS

DATE

March 2026 M3

WORK PACKAGE

WP4

LEADER

W4C

DISSEMINATION LEVEL

Public

TYPE

Document, report

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

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 European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Authors	Organisation
Camille Montmorency	**W4C**
Deniz Özer	**BV**

Peer Reviews	Organisation
Vanesa Daza	**UPF**
Saša Grašič	**UM**
Florence Sedes	**UT**

Revision History

VERSION	DATE	REVIEWER	MODIFICATIONS
1.0	**08/03/2026**	**Vanesa Daza (UPF)**	**First version**
1.0	**13/03/2026**	**Saša Grašič (UM)**	**Changed UM as task lead for D1.3 in chapter 6**
2.0	**20/03/2026**	**Camille M. (W4C)**	**Applied reviewers comments**
2.1	**24/03/2026**	**Camille M. (W4C)**	**Minor revisions**
2.2	**31/03/2026**	**Camille M. (W4C)**	**Updated exploitation plan**
2.3	**31/03/2026**	**Camille M. (W4C)**	**Final version**

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

ABBREVIATIONS AND ACRONYMS

Abbreviation	Meaning
BV	Bilişim Vadisi
CEFCYS	Le Cercle des Femmes dans la Cybersécurité
CEPS	Centre for European Policy Studies
CSA	Coordination and Support Action
DESCA	Development of a Simplified Consortium Agreement
DISCOM	Dissemination & Communication & Exploitation
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
IACR	International Association for Cryptologic Research
ICT	Information and Communication Technology
IPR	Intellectual Property Rights
ISACA	Information Systems Audit and Control Association
ISC2	International Information System Security Certification Consortium
KPI	Key Performance Indicator
MoU	Memoranda of Understanding
PEDR	Plan for Exploitation and Dissemination of Results
SME	Small and Medium sized Enterprises
STEM	Science, Technology, Engineering and Mathematics
UM	Univerza v Mariboru
UPF	Universitat Pompeu Fabra
UT	Université de Toulouse
W4C	Women4Cyber
WiCys	Women in Cybersecurity

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

CONTENTS

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

INDEX OF TABLES

INDEX OF FIGURES

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

EXECUTIVE SUMMARY

This deliverable presents the Dissemination, Communication and Exploitation (DISCOM) Plan of the WEM Cyber project (Widening Excellence and Mentoring in Cybersecurity). It establishes a structured and operational framework to ensure that project activities, opportunities, outputs and results are communicated effectively, disseminated strategically and exploited sustainably throughout the project lifecycle.

WEM Cyber addresses the persistent underrepresentation of women in cybersecurity and the structural barriers affecting skills development and career progression, particularly in Widening countries. Through structured secondments, mentoring and tailored training, the project strengthens cross-sectoral and cross-border collaboration between academia, industry and civil society, contributing to a more inclusive and resilient European cybersecurity ecosystem.

The plan defines:

- Target audiences and tailored key messages.
- Communication channels, including the project website, social media platforms, newsletter and partner networks.
- A structured press and editorial approach.
- Participation in events and stakeholder engagement activities.
- A coherent visual identity aligned with accessibility principles.
- Mandatory EU visibility and funding acknowledgement requirements.
- A comprehensive KPI framework to monitor performance and impact.
- A structured exploitation strategy focused on knowledge transfer, institutional uptake and long-term sustainability.

Overall, the DISCOM plan provides a practical, measurable and adaptable roadmap to maximise the visibility, reach, credibility and sustainability of WEM Cyber.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

1. INTRODUCTION

WEM Cyber (Widening Excellence and Mentoring in Cybersecurity) addresses the persistent underrepresentation of women in the cybersecurity field and the structural challenges that affect skills development and career progression. The project responds to the growing demand for cybersecurity expertise across Europe and to the need for more inclusive and balanced participation in a highly strategic sector.

The project implements structured secondments, mentoring and tailored training activities that promote cross-sectoral and cross-border collaboration between academia and industry, with a particular focus on Widening countries. These activities are designed to support knowledge exchange, enhance both technical and transversal skills, and encourage long-term professional networks that extend beyond the project duration.

The project brings together a multidisciplinary consortium composed of academic institutions, industry-oriented organisations and civil society actors with recognised expertise in cybersecurity, education, gender equality and innovation ecosystems. This combination enables WEM Cyber to bridge academic research and practical application, while also addressing structural barriers that limit women's participation and progression in the field.

2. DISSEMINATION AND COMMUNICATION OBJECTIVES

The DISCOM objectives of WEM Cyber define the contribution of dissemination and communication to the achievement of the project's main objectives. The core pillars of the DISCOM plan are to:

1. **Deliver high-quality and consistent communication**, making project information, opportunities and progress accessible to audiences throughout the project lifetime.
2. **Engage with identified target audiences**, including women in cybersecurity, academia, industry, civil society and other relevant stakeholders, through tailored approaches and formats.
3. **Disseminate project outputs, experiences and lessons learned**, positioning project knowledge as a resource that can support exchange and learning beyond the consortium.
4. **Highlight cross-border collaboration**, reflecting the project's aim to connect actors across different countries and sectors.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

This section defines the communication focus and key-message orientation for each audience and summarises these elements in a structured overview to ensure consistency between objectives, audiences and communication choices.

The project will also establish collaborations with leading women in cybersecurity organisations, such as CEFCYS, in order to strengthen outreach, promote gender diversity, and leverage synergies at European level.

3. TARGET AUDIENCES

WEM Cyber addresses a diverse set of target audiences, identified in the project proposal, including groups directly involved in or benefiting from project activities and wider stakeholder groups.

This section defines the communication focus and key-message orientation for each audience and summarises these elements in a structured overview to ensure consistency between objectives, audiences and communication choices.

3.1. Key messages

DISCOM key messages are guided by a consistent positioning that reflects the project's purpose, activities and expected contribution to cybersecurity skills and inclusion in Europe. Rather than relying on promotional language, communication is opportunity-driven, evidence-based, and inclusive, positioning WEM Cyber as a practical European initiative that creates concrete opportunities for women in cybersecurity.

The project's general key messages provide a shared foundation for all communication and dissemination actions. They are designed to be reusable across formats and audiences while remaining adaptable in emphasis depending on context. Together, they express how WEM Cyber supports participation, cooperation, skills development and inclusive career pathways in cybersecurity.

- WEM Cyber creates real entry points into cybersecurity through secondments, mentoring and tailored training that build skills and open career opportunities.
- Across Europe, WEM Cyber connects organisations from different sectors to share knowledge, develop talent and work together on cybersecurity challenges.
- Cybersecurity in Europe needs more skilled and diverse professionals, and WEM Cyber supports women with hands-on learning and cross-sector experience.
- WEM Cyber enables people, skills and ideas to move between academia, industry and society, turning knowledge into real-world cybersecurity capacity.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Supporting women's careers in cybersecurity strengthens innovation, resilience and expertise across the European digital ecosystem.

3.2. Tailored communication focus

The table below summarises the project's target audiences as defined in the proposal and outlines, for each audience, the main communication focus, and the orientation of key messages.

Table 1 - Tailored messaging

Target audience	Strategic driver / audience need	Tailored key message	Main channel
Women in cybersecurity and STEM	Access to concrete opportunities, skills development and career progression in cybersecurity.	**WEM Cyber creates real entry points into cybersecurity through secondments, mentoring and tailored training that build skills and open career opportunities;** Participation in WEM Cyber provides practical experience, professional connections and clearer pathways into long-term cybersecurity careers.	Website; social media; newsletter; webinars
Academic institutions and research organisations	Collaboration, knowledge exchange and capacity building that can be sustained or replicated.	**Across Europe, WEM Cyber connects organisations from different sectors to share knowledge, develop talent and work together on cybersecurity challenges;** The project offers mentoring, training and secondments that institutions can adapt within their own programmes and partnerships.	Website; publications; partner networks

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Cybersecurity industry and private sector	Access to skilled talent, practical collaboration and application of knowledge in real-world contexts.	**WEM Cyber enables people, skills and ideas to move between academia, industry and society, turning knowledge into real-world cybersecurity capacity;** Engagement with the project supports recruitment pipelines and emerging talent trained through cross-sector experience.	Website; events; social media; partner networks; newsletter
Policymakers and government agencies	Insight into skills needs, gender inclusion and effective approaches to strengthening cybersecurity capacity.	**Cybersecurity in Europe needs more skilled and diverse professionals, and WEM Cyber supports women with hands-on learning and cross-sector experience;** Project results provide evidence, tested practices and policy-relevant insights to inform inclusive cybersecurity skills strategies at national and European levels.	Website; publications; policy events; press
Non-governmental organisations and advocacy groups	Resources, collaboration and visibility to support gender equality and inclusion in cybersecurity.	**Supporting women's careers in cybersecurity strengthens innovation, resilience and expertise across the European digital ecosystem.** WEM Cyber offers collaboration opportunities, shared resources and visibility that reinforce ongoing advocacy and	Website; partner networks; social media; events; webinars

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

		community-driven inclusion initiatives.	
General audience	Basic awareness of cybersecurity's importance and the role of women in the field.	Cybersecurity in Europe needs more skilled and diverse professionals. WEM Cyber highlights real stories, accessible learning pathways and inclusive participation in cybersecurity careers.	Website; social media; webinars

4. PROPOSED ACTIVITIES AND CHANNELS

The following section outlines the main communication channels that will be used to ensure consistent visibility, effective dissemination, and broad outreach of WEM Cyber activities and results throughout the project.

4.1. Main communication channels

4.1.1. Website

The WEM Cyber website will be the central communication and information hub of the project, a reference point where stakeholders can access accurate, up-to-date and structured information about the project's objectives, activities and results. All other communication channels will direct audiences back to the website with an .eu domain. It will be maintained continuously throughout the project. Updates will occur regularly to reflect news, events and new opportunities, at key milestones such as the publication of results, and whenever necessary to ensure consistency. Responsibility for content coordination will lie with the dissemination lead, with contributions from all partners according to their respective activities and outputs.

Currently, the website is under development. In the meantime, a WEM Cyber webpage is hosted on the Women4Cyber Foundation's website for visibility:

https://women4cyber.eu/wemcyber/7

The website will follow a clear and user-oriented architecture designed to support intuitive navigation and differentiated stakeholder needs. An indicative structure includes:

- **Home** — Overview of the project, latest updates and key highlights.
- **The project**

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- About us, call ID, project summary, objectives, impact
- Consortium, partner organisations and their roles, affiliated entities
- Sister initiatives

- **Results**
  - Digital repository with press, newsletters, videos, downloadable materials
  - Gallery with all deliverables
- **Activities**
  - International secondments, success stories
  - About mentoring and training
  - Knowledge transfer platform
- **News & Events** — blog, updates on milestones, events, webinars
- **Get involved** — contact form
- **FAQ** – most frequently asked questions about the project

This structure may evolve during implementation to reflect project needs.

From M8 onwards, the Knowledge Transfer Platform (D3.7), led by UBITECH, will serve as a central repository and collaborative hub for research outputs, secondment-related materials, training resources and best practices generated during the project. The project website, social media channels, newsletters, webinars and events will be used to drive traffic to the platform and promote the uptake and reuse of its contents by both consortium partners and external stakeholders.

4.1.2. Social media

Social media channels will ensure continuous visibility and dissemination of WEM Cyber activities and results from the earliest stage of the project until its conclusion. Dedicated project accounts have been created on LinkedIn, YouTube, Facebook and Instagram, complementary in reaching target audiences. We are also planning to open an X (former Twitter) account.

Official project accounts

LinkedIn

Instagram

Meta / Facebook

YouTube

Content will combine information, narrative and engagement-driven approaches to attract attention, sustain interest and guide audiences toward concrete opportunities within the

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

project. Communication will highlight secondments, mentoring, training activities, calls for participation and deadlines; knowledge platform; storytelling and success stories featuring participants and their experiences; and lessons learned and project achievements in accessible formats. Recurring formats structure this activity, including short news updates, participant or mentor spotlights, event-related communication, and infographics presenting project themes, and results derived from partners' activities. Thematic posts related to cybersecurity skills, careers and inclusion will further enhance the outreach.

Additionally, we plan to provide partners with a social media toolkit containing ready-to-publish templates, recommended hashtags and keywords, as well as communication guidelines to support consistent and effective promotion of the project.

4.1.3.Newsletter

The WEM Cyber newsletter will be a direct communication tool to inform stakeholders, to provide periodic and summarised updates, and to bring together key developments in a single, accessible format. The newsletter will be distributed with Brevo, a platform which enables the sender to segment audiences and monitor performances. The subscription form will be accessible on the project website and promoted through social media, events and partner networks.

The newsletter will be sent out every three months starting from M6. This ensures continuity of communication while allowing sufficient time to gather meaningful updates, results and opportunities. Additional special editions may be released when significant milestones or key project results justify targeted communication. Content will prioritise clarity and actionability**,** for readers to quickly identify opportunities and access further information through links to the project website.

4.1.4. Content

The project will release at least two short videos: one to introduce WEM Cyber, and another one to explain why increasing women's participation in cybersecurity matters for digital resilience, and position WEM Cyber as a practical initiative addressing this gap. Both videos are intended for reuse across the project website, social media, presentations and awareness campaigns. In addition, a series of at least three videos will be produced, each one to address a clear question relevant to the target audiences, for instance how to enter cybersecurity from different backgrounds, what skills are needed in real professional roles, and how secondments contribute to career development. The content will rely on concrete experiences from project activities.

Content formats will be adapted on each platform. Professional-oriented messaging and event visibility are prioritised on LinkedIn, concise real-time updates and campaign

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

interaction on Instagram, accessible community-focused communication on Facebook, and longer-formats on YouTube. This platform-sensitive approach ensures coherence of messaging while optimising reach and accessibility across diverse audience groups.

Targeted communication campaigns will also be organised around major project milestones and relevant international awareness moments, as shown in the table below. Consortium partners will further amplify the outreach through their own accounts, extending dissemination across national contexts and professional communities.

Table 2 – International days and project milestones calendar

Date	Opportunity	Relevance / communication focus
24 January	International Day of Education	Connects cybersecurity skills, lifelong learning and access to training with the project's mentoring and capacity-building approach.
28 January	Data Privacy Day	Direct link to cybersecurity awareness, data protection and trust in digital environments.
February (variable)	Safer Internet Day	European-level awareness moment connecting digital safety, education and responsible technology.
11 February	International Day of Women and Girls in Science	Highlights women's participation in STEM and cybersecurity, mentoring pathways and inclusive career opportunities promoted by the project.
8 March	International Women's Day	Major annual visibility moment to showcase women's careers in cybersecurity, participant stories and mentoring impact.
Fourth Thursday of April	Girls in ICT Day	Raises awareness of digital and cybersecurity career pathways among younger generations and future talent pipelines.
9 May	Europe Day	Emphasises European cooperation, cross-border secondments and shared capacity building in cybersecurity across Widening countries.
May–June (variable)	European Semester Spring Package	Opportunity to align project messaging with EU cybersecurity, research and skills policy discussions.
July - August	Summer holidays	Minimal but consistent presence and reminders of opportunities during quieter holiday period.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

18 September	International Equal Pay Day	Connects gender equality, career progression and inclusive participation in cybersecurity professions.
Last Friday of September	European Researchers' Night	Strong academic outreach opportunity linking research careers, mobility and knowledge exchange with cybersecurity excellence.
October (full month)	European Cybersecurity Awareness Month	Primary annual campaign peak fully aligned with project scope: cybersecurity awareness, skills, careers, diversity and dissemination of results.
October (variable)	EU Code Week	Promotes digital skills, education and pathways into technology careers relevant to cybersecurity capacity building.
December	Year-end wrap-up and new-year	Summarises achievements and future opportunities.

4.2. Stakeholder engagement

4.2.1. Events

WEM Cyber consortium partners will participate in European and national conferences and industry events where cybersecurity skills development, diversity in technology and cross-sector collaboration are actively discussed. Participation formats may include presentations of project activities and results, panel discussions or meeting with stakeholders. Beyond visibility, this type of engagement will support networking, knowledge exchange and community building**.** Direct interaction with researchers, practitioners, industry representatives and policymakers will facilitate dissemination of project insights, identification of collaboration opportunities and broader recognition of WEM Cyber's contribution to inclusive cybersecurity skills development in Europe. A consolidated overview of relevant events is provided in **Annex 1 - Relevant conferences, events and initiatives** and may be updated during project implementation where appropriate.

4.2.2. Webinars

Webinars will be used as a dedicated stakeholder engagement format to reach academic, industry and policy audiences across Europe in an accessible and scalable way. At least three webinars will be organised during the project, in online or hybrid format, and will address topics such as secondment opportunities, mentoring and training activities, women's careers in cybersecurity, project results, and the Knowledge Transfer Platform.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Webinars will be scheduled in connection with key project milestones and will support both dissemination and the uptake of project outputs.

Particular attention will be given to balanced and diverse representation among speakers, including gender balance, diversity of professional and cultural backgrounds, and representation across countries and sectors.

4.3. Dissemination

4.3.1. Publications

The publication of articles in academic journals or industry publications will enhance the credibility of the research performed during the secondments as well as highlight the scientific and practical achievements of the project, ensuring that knowledge generated within WEM Cyber becomes accessible to research, education and professional communities beyond the consortium.

Responsibilities will lie with the partners directly involved in the underlying research or activity, while the DISCOM lead will ensure coherence of acknowledgements and alignment with project aims.

Relevant publication venues include, but are not limited to, the following:

- Elsevier cybersecurity and information-security journals
- IACR conference proceedings and cryptography-related publications
- Privacy & Data Protection Journal
- Taylor & Francis journals covering cybersecurity, digital governance and education
- Peer-reviewed, professional and/or industry publications addressing applied cybersecurity practice, policy implementation, digital skills, STEM education, gender balance, and innovation ecosystems

4.3.2. Press release and media outreach

Press releases will be prepared and issued based on factual input provided by the partners responsible for the relevant activity or result. Each press release will function as a documentary record of project developments, presenting verified information, contextualising the activity or outcome, and providing a reliable reference for journalists, institutions and stakeholders. Press releases are therefore not intended to generate demand or promotional attention, but to ensure accurate public documentation of the project's implementation and results.

Press releases will be published on the project website and LinkedIn account, relayed through partners channels, and shared with relevant press outlets when appropriate. Press

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

releases will be considered at key stages of the project lifecycle where results or progress justify formal public documentation. These stages may include:

1. Kick-off meeting and official launch of the WEM Cyber project: **Annex 2 – First Press release**
2. Opening of the first secondment call.
3. Start of mentoring activities and training programme.
4. Completion of the first secondment cycle and initial outcomes from participants.
5. Consolidation of mid-term progress, including participation levels and emerging lessons
6. Launch of subsequent secondment or training phases.
7. Publication of significant collaborative research or methodological outputs.
8. Initial results of mentorship and coaching activities.
9. Launch of knowledge transfer platform.
10. Formal closure of the project, overall impact and future perspectives.

The project also aims to generate at least forty media or news articles over its duration. To support this target, partners should be publishing short news articles on the project website on a regular basis, for example once a month, complemented by additional articles whenever significant project developments occur. Among the topics that could be developed are:

- Emerging cybersecurity career paths.
- Common misconceptions about working in cybersecurity.
- Day-in-the-life perspectives from professionals across sectors.
- Portrait from Consortium partner or secondee.
- What skills matter more than coding in cybersecurity
- Changing careers to cybersecurity after 30
- Big data security and analytics
- Cyber-threat intelligence
- Blockchain and DLT security
- Etc.

This editorial content will contribute to increasing traffic to the project website, as each article will be relayed through the project's social media channels.

4.4.Partners' network and local impact

Consortium partners will play an active role in disseminating project information and results through their own communication channels and professional networks. This

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

includes engagement with initiatives active in cybersecurity, gender equality and STEM. Through existing connections with women in STEM initiatives, the consortium has access to a broad European ecosystem, including the network of Women4Cyber chapters across Europe, as well as organisations such as **ISC2**, **GFCE**, **ISACA**, **WiCyS**, **CEPS**, **Women in Engineering**, **CEFCYS** and **Femmes & Sciences**, among others.

An overview of partner communication channels is provided in **Annex 3 – Partner communication channels**, which may be updated during project implementation where relevant.

DISCOM activities are coordinated at project level by Women4Cyber as leader of Work Package 4 on Communication and Dissemination. Consortium partners will contribute by providing knowledge input and updates to inform content creation. This shared approach will ensure strong impact across all DISCOM channels.

5. VISUAL IDENTITY

The WEM Cyber visual identity was created during the first two months of the project and will be consistently applied across all dissemination and communication activities. This includes the development of branded materials such as document templates, one pager, the project website, roll-up banners, videos, and other promotional assets produced within the framework of the project.

The WEM Cyber brand identity **Annex 4 – Branding booklet** is defined by a set of distinctive visual and stylistic components, including its colour palette, fonts, logo, and overall design language, that ensure immediate recognition and strong association with the project. Its development was based on a comprehensive analysis of the project's objectives and context, alongside a careful evaluation of its core values.

As part of the branding process, three distinct logo concepts were designed and presented to the consortium for consideration, as shown in the visuals below. Following internal discussion and voting, the final logo was selected through a majority vote and the design #3 was chosen.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Figure 1 – Logo design #3 and applications

Figure 2 – Logo designs #1 and #2

The visual identity of WEM Cyber is built around a modern and approachable representation of innovation in cybersecurity.

The main logo combines a minimalist profile of a woman with interconnected nodes and dots, symbolising digital networks, knowledge exchange and tech. The use of lowercase typography reinforces accessibility and inclusiveness, positioning the project as open and collaborative.

The colour palette is deep blue (#1a1f73), vibrant green (#a5f257), purple (#ab62cd) and neutral grey (#9a9a95). The choice of Poppins as the main font ensures clarity and consistency across digital and print materials.

Together, these elements establish a distinctive identity that reflects both the technical focus of cybersecurity and the project's commitment to supporting women in the field.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

5.1. Accessibility

The visual identity of WEM Cyber is designed to support clarity, coherence and accessibility across all materials.

Clean typography, structured layouts and high-contrast colour combinations ensure readability in both digital and print formats. Templates are developed with accessibility principles in mind, including clear hierarchy, legible font sizes, consistent spacing and compatibility with assistive technologies where applicable. The objective is straightforward: materials must be easy to navigate, visually coherent and usable by all audiences, including people with disabilities.

DISCOM activities follow a clear, respectful and professional tone. Messages are written to be understandable to audiences with varying levels of cybersecurity expertise, from researchers and industry professionals to students, policymakers and general stakeholders. Unnecessary jargon, buzzwords and exaggerated promotional language are deliberately avoided. Instead, communication prioritises precision, factual clarity and transparency about what the project does and delivers.

WEM Cyber is positioned around concrete opportunities and measurable actions, rather than abstract statements or deficit-based narratives. The project does not frame women's participation in cybersecurity as a problem to be fixed, but as a capability to be strengthened and supported.

Language is inclusive and gender-sensitive, and representation reflects diversity not only in gender but also in professional background, geography and career stage. Across all outputs, women in cybersecurity are presented through their expertise, leadership and contributions, reinforcing agency and competence rather than focusing on gaps or underrepresentation alone.

5.2. Mandatory guidelines

According to Article 17 of WEM Cyber Grant Agreement, it is worth highlighting the following requirements that the project will comply with during the implementation of all DISCOM activities.

Unless otherwise agreed with the granting authority, communication activities of the beneficiaries related to the action (including media relations, conferences, seminars, information material, such as brochures, leaflets, posters, presentations, etc., in electronic form, via traditional or social media, etc.), dissemination activities and any infrastructure, equipment, vehicles, supplies or major result funded by the grant must acknowledge EU

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

support and display the European flag (emblem) as shown below and funding statement (translated into local languages, where appropriate).

Figure 3 -EU funded emblems

The emblem above must remain distinct and separate and cannot be modified by adding other visual marks, brands, or text. All emblems can be downloaded from here: **https://ec.europa.eu/regional_policy/information-sources/logo-download-center_en**

When displayed in association with other logos (e.g., of beneficiaries or sponsors), the emblem must be displayed at least as prominently and visibly as the other logos.

For the purposes of their obligations under Article 17, the beneficiaries may use the emblem without first obtaining approval from the granting authority. This does not, however, give them the right to exclusive use. Moreover, they may not appropriate the emblem or any similar trademark or logo, either by registration or by any other means.

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):

"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 European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them."

6. EVALUATING SUCCESS

6.1. Consolidated KPIs

The table below gathers the quantitative DISCOM indicators defined in the project proposal. Progress will be reviewed at M12, M24 and M36 to check whether activities remain on track and to identify gaps early enough to react.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

For monitoring purposes, the size of the online community refers to the cumulative number of followers and subscribers across the project's official social media accounts and newsletter database.

Table 3 - DISCOM KPIs

Area	Indicator	Target value	Responsibility	M12	M24	M36
Social media	Instagram followers[1]	+250	W4C			
	YouTube followers	+120	W4C			
	LinkedIn followers	+900	W4C			
	Size of online community	+1000	W4C			
Events	Major events attended	+8	All partners			
	Industry events attended	+5	All partners			
	Local / national meet-ups	+10	All partners			
	Webinars organised	+3	W4C + partners			
Website	Monthly unique visitors (avg.)	+800	W4C			
	Monthly returning visitors (avg.)	+400	W4C			
	Monthly page views	+1500	W4C			
Media & press	Media articles	+40	W4C + partners			
	Press releases	+10	W4C			
Mailing / newsletter	Campaigns sent	10	W4C			
	Average open rate	20%	W4C			
Publications	Academic publications	29	WP2			
	Including joint publications	+8	WP2			
Geographic reach	Widening countries directly reached	4	All partners			
	EU countries directly reached	7	All partners			

[1] The proposal sets a KPI of +250 followers on X. We recommend shifting this to Instagram.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

	EU countries indirectly reached	+30	All partners			
Network	Connections with cybersecurity initiatives	+15	All partners			

6.2. Monitoring

Reaching the agreed numbers of major events, industry events and national or local meet-ups requires continuous follow-up from the beginning of the project rather than retrospective counting at reporting stages. To organise this follow-up in a simple and workable way, the project will maintain a shared spreadsheet accessible to all partners (with event name, date, location, format, partner attending, participation status). Tracking alone is not sufficient to guarantee participation. For this reason, we will circulate a short mailing every quarter to present upcoming events and invite partners to confirm attendance where opportunities remain open.

Connections with cybersecurity, STEM and gender-equality initiatives will be monitored with the same level of attention as event participation, as they contribute directly to the project target of establishing at least fifteen collaborations with external initiatives. Another tab can be added to the spreadsheet to record each interaction with organisations beyond the consortium. For every entry, the tracker specifies the organisation involved, type of interaction (joint event, panel invitation, knowledge exchange, partnership discussion), date, partner responsible, etc. This will be aligned with the same quarterly follow-up used for event participation.

When gaps appear, such as limited interaction or insufficient progress toward the target KPI, follow-up actions will be initiated. These may include activating partners' national networks, proposing joint visibility actions, inviting external organisations to webinars or events, or formalising ongoing exchanges into documented collaboration.

Geographic reach will be assessed using information collected during project activities. Country data can be collected through applications to secondments, mentoring and training activities, webinar and event registrations. Bringing these sources together makes it possible to identify the countries directly involved in activities from EU countries and Widening countries. For other indirect KPIs, analytics reports will be downloaded to provide evidence of dissemination reach for social media, newsletter and website statistics.

Monitoring remains continuous throughout the project and allows dissemination activities to be adjusted when needed. This keeps progress toward WEM Cyber commitments visible, documented and under control across the full implementation period.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Once operational, the Knowledge Transfer Platform will also be monitored through usage indicators such as visits, registered users, uploaded resources, downloads and user feedback, in order to assess its contribution to knowledge sharing, dissemination and exploitation.

7. EXPLOITATION

The exploitation strategy will be developed and coordinated by BV, as project coordinator, in line with Task 4.3 of the Grant Agreement, with contributions from all partners.

The WEM Cyber project, as a Coordination and Support Action (CSA), aims to strengthen the European cybersecurity and trustworthy AI ecosystem by harmonising strategic collaborations and enhancing capacity building among key stakeholders. Our exploitation strategy ensures that project results are not only disseminated but also systematically adopted (uptake) and institutionalised by both academic and industrial partners beyond the project duration.

7.1. Exploitation Strategy

The project's exploitation approach focuses on ensuring that the developed training content, digital tools, and collaboration models are effectively used and sustained beyond the project duration. The primary target groups include **PhD candidates, postdoctoral researchers, academic institutions, and industry partners.**

The project addresses **the gap between research and market** by strengthening innovation and entrepreneurial skills, particularly in the fields of cybersecurity and trustworthy AI. Exploitation will be achieved through the **integration of project outputs into educational programmes, continued use of digital tools, and the establishment of long-term collaborations between academic and non-academic partners.**

7.2. IPR and Ownership

The Consortium Agreement is based on the DESCA model[2], ensuring a balanced framework for intellectual property management and partner responsibilities, consistent with Section 2.2.2 of the proposal.

All project outputs will be managed in line with the consortium agreement, ensuring a balance between accessibility and the protection of intellectual property rights. Training

[2] https://intellectual-property-helpdesk.ec.europa.eu/ip-management-and-resources/publications/model-consortium-agreement-desca-horizon-europe-20_en

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

materials and non-sensitive outputs will be shared among partners, while respecting applicable data protection and ownership principles.

7.3. Monitoring and Evaluation

Exploitation activities will be monitored by a designated Exploitation Manager through the Plan for the Exploitation and Dissemination of Results (PEDR), which will be updated periodically to track progress against the measurable and contractual KPIs in the exploitation table.

Table 4 – Exploitation Plan and related KPIs

Section	Exploitation Actions / Outputs	Stakeholders	KPIs / Impact (CSA Scale)
Training Programs	Academic partners will integrate pilot modules into postgraduate curricula and continuing education offerings (short courses, executive programmes); non-academic partners will incorporate tailored training into professional development tracks for staff	Academic partners, industry staff	• At least 10 technical and soft-skill training sessions delivered. • Up to 37 professional certifications obtained by secondees. • Participant satisfaction rate of at least 80%, measured via post-programme surveys.
Project Assets	These outputs encompass proof-of-concept tools, methodological frameworks, training resources, and research publications resulting from secondment activities, which represent the main knowledge-based results of the project and form the	Academia, SMEs, local institutions, industry partners	• At least 29 research publications, of which a minimum of 8 shall be joint publications co-authored between academic and non-academic partners. • Contribution to at least 10 new cybersecurity tools, prototypes, or applied solutions developed during secondment research.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

	basis for further use, adaptation, and potential scaling.		• At least 3 training modules or curricula resources validated and available for integration into postgraduate or professional programmes. • 100% of publications made available through Open Access channels, including Open Research Europe.
Digital Collaboration Platform	Maintain a digital platform enabling knowledge exchange, matchmaking, and resource sharing.	All partners and participants	• +40 downloads • +30 uploaded content • Platform guaranteed to be active at least 2 years post-project. • Platform access visits: at least 1,000 during the project lifetime. • Contribution rate: at least 70% of participating organisations actively upload content.
Collaboration & Sustainability	Establish formal agreements (Memoranda of Understanding, joint supervision frameworks, or co-funding commitments) between academic and non-academic partners to sustain joint research initiatives, internship schemes, and mobility programmes b eyond the project lifecycle.	Academic & non-academic partners	• At least 5 formal collaboration agreements (MoUs or equivalent instruments) signed between consortium partners, each specifying joint activities planned for a minimum of 24 months post-project. • At least 2 joint research proposals or co-funding applications submitted by consortium partners by M36.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

		• Establishment of at least 1 structured internship or mobility scheme formalised betwe en a widening-country partner and a non-widening-country partner.

This exploitation strategy (D4.1, M3) will be updated in D4.2 (M12) and finalised in D4.3 (M36), with full exploitation activities developed under Task 4.3 from M25 onwards.

8. GDPR AND DATA PRIVACY

Respect for privacy and the protection of personal data are essential principles guiding all DISCOM activities carried out within WEM Cyber. Consortium partners ensure that any collection, use or storage of personal data during project activities complies with the General Data Protection Regulation (GDPR) and with the internal data-protection procedures of their respective organisations.

When images, recordings, or other personal data are collected during events, webinars, surveys or related activities, participants are informed in advance about the nature and purpose of the data collection, the conditions of processing, the storage period and their rights regarding access, correction or withdrawal of consent. Explicit consent is obtained where required, including for the capture and use of photographs in DISCOM outputs.

Each partner remains responsible for the lawful processing and secure handling of personal data under its control and ensures that project-related data are managed through authorised institutional systems rather than personal accounts or informal storage solutions. Communication with external contacts is conducted in a responsible manner, and project information is shared only with recipients who have provided appropriate consent to receive such communications.

A privacy policy will be published on the project website, clearly explaining how personal data related to website use, subscriptions or communication activities are collected, processed, stored and protected, in accordance with GDPR requirements.

Further details on research data management, data sharing, repository use, access levels and open access provisions will be specified in D1.3 Data Management Plan (lead beneficiary: UM, due in M6).

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

9. CONCLUSION

The WEM Cyber DISCOM Plan provides a coherent and actionable framework to ensure that communication, dissemination and exploitation activities are implemented in a structured, transparent and results-oriented manner.

By aligning key messages, target audiences, communication channels and measurable indicators, the plan guarantees consistency across consortium actions while allowing flexibility to respond to emerging opportunities, policy developments and stakeholder feedback. The approach prioritises opportunity-driven communication, reflecting the project's commitment to strengthening women's participation in cybersecurity through concrete and measurable actions.

Through coordinated communication efforts, active stakeholder engagement, structured dissemination of results and strategic exploitation of knowledge assets, WEM Cyber aims not only to deliver project outputs but to create sustainable impact.

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

10. ANNEXES

Annex 1 – Relevant conferences, events and initiatives

MAJOR EU WIDE EVENTS	NATIONAL EVENTS
Large cybersecurity forums and expos	Belgium
One Conference **https://one-conference.nl/** it-sa Expo & Congress **https://www.itsa365.de/en/it-sa-expo-congress** Cyber Security & Cloud Expo Europe (TechEx) **https://cybersecuritycloudexpo.com/europe/**	Security Forum (Digital First) **https://digitalfirst.be/security-forum/** Data Protection & Privacy Conference **https://www.cpdpconferences.org/about-cpdp** Cybersec Europe **https://www.cyberseceurope.com/**
Policy and standards	France
European Cybersecurity Standardisation Conference (ENISA) European Cybersecurity Skills Conference (ENISA) European Cybersecurity Certification Conference (ENISA) **https://www.enisa.europa.eu/events**	Cyber/IA expo **http://ia-cyber.com/** Forum InCyber **https://europe.forum-incyber.com/en/home-en/** ETSI Security Conference **https://www.etsi.org/events/2481-etsi-security-conference-oct2025**
Skills and diversity in STEMS	Greece
Women4Cyber Cybersecurity Conference **https://women4cyber.eu/** CyberSQUAD **https://www.connect2trust.nl/cybersquad-2025/**	InfoCom Security **https://www.infocomsecurity.gr/en/** IEEE CSR **https://www.ieee-csr.org/**

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

European Cybersecurity Challenge **https://ecsc.eu/**	
	Lithuania / Baltics
	Baltic Security Conference **https://balticsecurityconference.lv/en/** Cyber Chess **https://cyberchess.lv/**
	Slovenia
	INFOSEK **https://www.infosek.net/en**
	Spain
	Cybersecurity Congress **https://www.barcelonacybersecuritycongress.com/** ENISE International Information Security Meeting **https://www.incibe.es/en/events/enise**
	Türkiye
	UPSchool Events **https://www.upschool.io/** Cyber Security Summit **https://security.devnot.com/** ENBANTEC Cyber Security Conference **https://www.enbantec.com/English.aspx** ISC Türkiye - International Conference on Information Security and Cryptology **https://iscturkiye.com/en/anasayfa-english/**

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Annex 2 – First press release

wem cyber

Funded by the European Union

PRESS RELEASE | 24.02.2026

WEM CYBER OFFICIALLY LAUNCHES IN ISTANBUL TO STRENGTHEN WOMEN'S PARTICIPATION IN CYBERSECURITY ACROSS EUROPE

The WEM Cyber project (Widening Excellence and Mentoring in Cybersecurity) officially launched last week on February 17, at its Kick-off Meeting hosted by Bilisim Vadisi in Istanbul.

Over two days, project partners gathered to align on objectives, implementation plans and collaboration mechanisms for the 36-month Horizon Europe initiative. The meeting marked the formal start of coordinated work to address gender imbalance in cybersecurity and to strengthen skills development and cross-sector collaboration across Europe.

The agenda included a detailed presentation of the project's objectives, deliverables, timeline and key performance indicators, followed by work package sessions covering project management, academia–industry secondments, entrepreneurship and employability enhancement, communication and dissemination, and ethics requirements.

Discussions focused on operational planning for the first project phase, including the implementation of structured secondments, mentoring activities and training actions designed to create practical entry points into cybersecurity careers. Particular attention was given to cooperation between academia and industry, ensuring that knowledge and skills circulate across sectors and countries. The second day of the meeting included a presentation on Communication and Dissemination, and Ethics Requirements.

"Today, we are not just launching a project, we are officially starting a 3-year mission. We call it WEM Cyber, but in reality, it is commitment to change the face of cybersecurity across Europe."

- Sezen Gungor, WEM Cyber Project Coordinator

WEM Cyber is funded under the Horizon Europe programme and brings together a multidisciplinary consortium committed to strengthening excellence and mentoring in cybersecurity, with a particular focus on Widening countries participation and supporting women's career progression in the field.

Consortium partners include:
- Bilişim Vadisi
- Boğaziçi University
- Vilnius Gediminas Technical University
- University of Maribor
- Universitat Pompeu Fabra
- Université Paul Sabatier Toulouse III
- Women4Cyber Foundation
- UBITECH

Affiliated entities include:
- SecroMix
- SphereTech
- CyberWhiz
- CloudMetrik
- Cyberware (Oninc)

Contact

Project Coordinator
Sezen Güngör, Director of International Relations, Bilisim Vadisi
coo.wemcyber@bilisimvadisi.com.tr

Press and Communication
Camille Montmorency, Project Manager, Women4Cyber Foundation
camille.montmorency@women4cyber.eu

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

https://heyzine.com/flip-book/2dc90aaed6.html

Annex 3 – Partners' communication channels

PARTNER ORGANISATION	ACTIVE CHANNELS & NUMBER OF FOLLOWERS (MARCH 2026)
Bilişim Vadisi Teknopark Yönetici A. Ş (BV)	**LinkedIn** 71.000 followers **Instagram** 41.300 followers **X** 47.400 followers
Boğaziçi University (BU)	**Facebook** 117.000 followers **Instagram** 2.800 followers **YouTube** 40.200 followers **LinkedIn** 170.000 followers
Vilnius Gediminas Technical University (VT)	**Facebook** 39.000 followers **LinkedIn** 53.000 followers **YouTube** 1.800 followers **Instagram** 1.200 followers
Univerza v Mariboru (UM)	**Facebook** 10.000 followers **Instagram** 1.000 followers **LinkedIn** 28.000 followers
Universitat Pompeu Fabra (UPF)	**LinkedIn** 179.000 followers **Instagram** 42.300 followers

Funded by the European Union

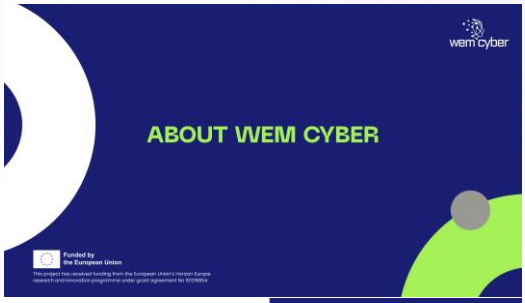
This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

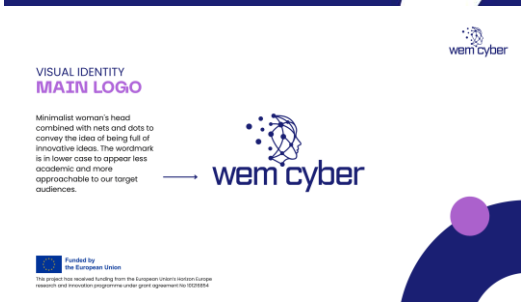
Université Toulouse III- Paul Sabatier (UT)	**YouTube** 2.100 followers **LinkedIn** 137.000 followers **Instagram** 15.600 followers **Facebook** 47.000 followers
Women4Cyber (W4C)	**LinkedIn** 25.700 followers **Instagram** 2.600 followers
Gioumpitek Meleti Schediasmos Ylopoiisi Kai Polisi Ergon Pliroforikis Etaireia Periorismenis Efthynis (UBITECH)	**LinkedIn** 10.000 followers **Instagram** 621 followers
AFFILIATED ENTITIES	
CyberWhiz	**LinkedIn** 1.650 followers
SphereTech	**LinkedIn** 1.000 followers
SecroMix	**Facebook** 102 followers **LinkedIn** 816 followers
CloudMetrik	**LinkedIn** 843 followers
Cyberware	**LinkedIn** 19 followers **Instagram** 41 followers

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Annex 4 – Branding booklet

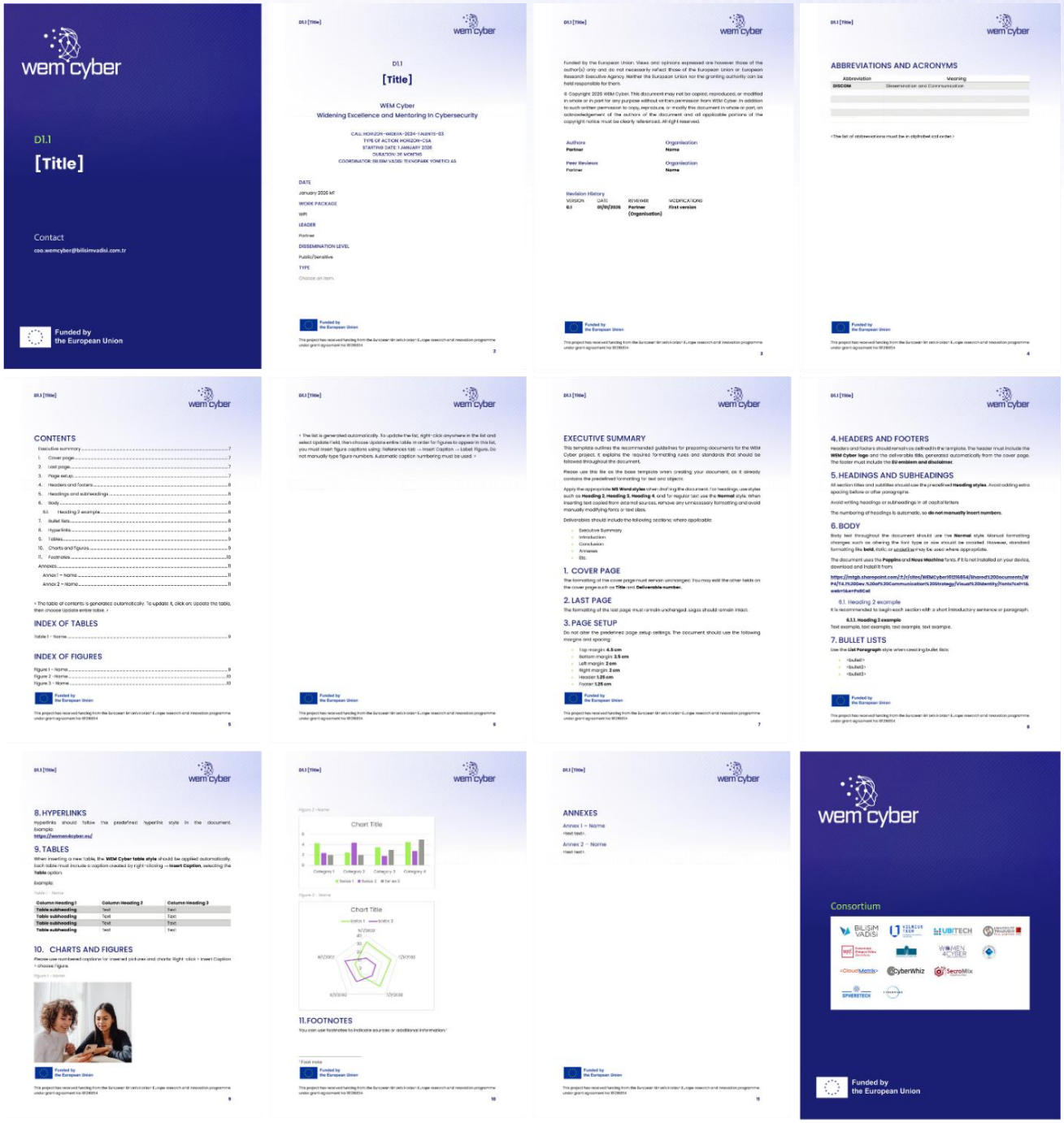




Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Annex 5 – Document template



Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Annex 6 – Presentation template

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Annex 7 – One pager

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

wem cyber

Consortium

BİLİŞİM VADİSİ

VILNIUS TECH
Fundamentinių mokslų fakultetas

UBITECH
ubiquitous solutions

Université de Toulouse

upf. Universitat Pompeu Fabra Barcelona

University of Maribor

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

BOĞAZİÇİ ÜNİVERSİTESİ 1863

<CloudMetrik>

CyberWhiz

SecroMix
#SeeWhat'sNext

SPHERETECH

CYBERWARE

Funded by
the European Union