



Co-funded by
the European Union



ECCE 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

DIGITAL-ECCE-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS

Grant Agreement number: 101128013



ERMIS: Cybersecurity Market Assurance and Insurance-As-A-Service

Deliverable D2.2 Report on Dissemination / Communication Activities

Deliverable release date	30/04/2025
Authors	<ol style="list-style-type: none">1. Insuretics2. ZELUS3. Sphynx4. Nodalpoint5. Karavias
Reviewer	Insuretics, NCSA
Deliverable Coordinator	Insuretics
Status of the Document	Draft
Version	1.0
Dissemination level	Public

Document Revision History

Version	Date	By	Description
0.1	06/03/2025	INSU	TOC creation
0.2	28/03/2025	INSU	Updated the TOC and allocate the sections to the partners
0.3	03/04/2025	ZELUS	Section 2, 4.2 and 4.4 writing
0.3	04/04/2025	SPH	Section 4.8
0.4	04/04/2025	NDP	Section 5.2
0.5	10/04/2025	INSU	Section 3, 4.1, 4.3, 4.5, 4.6, 4.7, 4.9, 5.3
0.6	11/04/2025	NDP	Updated Section 5.2
0.7	11/04/2025	INSU	Section 1, 6
0.8	28/04/2025	NCSA	First Review
0.9	28/04/2025	INSU	Second Review
1.0	30/04/2025	INSU	Final update and Editing

Acknowledgement

Co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Table of Contents

1.	List of acronyms and abbreviations	5
2.	List of Figures	6
3.	List of Tables.....	7
4.	Executive Summary	8
1.	Introduction	9
1.1.	Scope.....	9
1.2.	Document Structure	9
2.	Purpose and objectives.....	10
2.1.	ERMIS Impact Maximisation strategy	10
2.2.	Objectives	11
3.	Communication and Dissemination strategy	14
3.1.	Target groups and Audiences	14
3.2.	Communication Channels.....	15
4.	Communication and Dissemination Activities.....	16
4.1.	ERMIS Brand guide.....	16
4.1.1.	ERMIS LOGO	16
4.1.2.	ERMIS COLOURS.....	16
4.1.3.	DEVELOPMENT OF PROJECT TEMPLATES	16
4.2.	The funding information.....	16
4.3.	ERMIS Website	17
4.4.	Social Media	19
4.4.1.	LINKEDIN	19
4.4.2.	TWITTER/X	20
4.4.3.	YOUTUBE	21
4.4.4.	RESEARCH GATE / ZENODO	22
4.5.	Communication Material	23
4.5.1.	E-BROCHURE	23
4.5.2.	PROJECT PRESENTATION	24
4.5.3.	PROJECT BANNER.....	24
4.6.	Newsletters and Press Releases	27
4.7.	Workshops and Events.....	29
4.8.	Journal Publications, Scientific Papers and Conferences.....	31

4.9.	Communication Material - Dissemination Communication Exploitation (DCE) table.....	32
5.	Monitoring and Evaluation of Communication and Dissemination Activities	33
5.1.	Monitoring	33
5.2.	Reporting	33
6.	Conclusion	42
7.	Annex 1.....	43
8.	Annex 2	47

1. LIST OF ACRONYMS AND ABBREVIATIONS

Acronym	Description
CRIRM	Cyber Range, Insurance, and Risk Management
DCE	Dissemination, Communication, and Exploitation
DEP	Digital Europe Programme
DORA	Digital Operational Resilience Act
EU	European Union
FOSSA	Free and Open-Source Software Auditing
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
iKPI	Impact Key Performance Indicator
IT	Information Technology
KPI	Key Performance Indicator
NIS2	Network and Information Security 2 Directive
OSOR	Open-Source Observatory and Repository
Q&A	Question and Answer
SME	Small and Midsize Enterprises
WP	Work Package

2. LIST OF FIGURES

Figure 1. ERMIS “Home Screen Upper top”	18
Figure 2. ERMIS “Home Screen Bottom”	19
Figure 3. ERMIS LinkedIn account.....	20
Figure 4. ERMIS Twitter/X account	21
Figure 5. ERMIS YouTube account	22
Figure 6. ERMIS Zenodo first publication.....	23
Figure 7. ERMIS e-Brochure.....	24
Figure 8. ERMIS Zenodo first publication.....	26
Figure 9. Newsletter Issue #1	27
Figure 10. Newsletter Issue #2	28
Figure 11. Newsletter Issue #3	29
Figure 12. Agenda of the Workshop on Cyber Insurance and Cybersecurity.....	31



3. LIST OF TABLES

Table 1. Objectives and Key Actions 13

Table 2. Target Group Adoption of ERMIS Outcomes 14

Table 3. Funding Requirements 17

4. EXECUTIVE SUMMARY

This document presents a comprehensive overview of the communication and dissemination activities undertaken within the ERMIS project as part of WP2 during M1 and M18. The report outlines the project's multi-faceted strategy to maximise impact through strategic dissemination, targeted stakeholder engagement, and the development of reusable communication assets. The communication approach is aligned with the overarching project goals and is built upon four strategic pillars: mission-focus, openness, sustainability, and SME engagement.

The report details the identification of key audiences, channels used, and specific dissemination tools and events organised to date. Key accomplishments include the development of the ERMIS website, active social media presence, the release of newsletters and press releases, organisation of Info Days and workshops, and the production of project communication materials such as brochures and banners.

Monitoring and evaluation processes have been established to assess the effectiveness of these activities and adapt them in response to feedback and evolving project needs. The ERMIS consortium has also initiated steps towards long-term sustainability and exploitation of project outcomes through strategic partnerships and outreach. This deliverable demonstrates the consortium's strong commitment to fostering awareness, engagement, and adoption of ERMIS innovations across Europe.

1. INTRODUCTION

1.1. Scope

This deliverable outlines the dissemination and communication efforts of the ERMIS project up to Month 18. It presents the framework, activities, tools, and monitoring mechanisms employed to promote the project's objectives and outputs. The document aims to ensure transparency, stakeholder engagement, and optimal visibility of ERMIS's contribution to the European cybersecurity and cyber insurance ecosystem. Effective communication and dissemination are vital to fostering awareness, building trust, and encouraging adoption among diverse stakeholders, including regulators, SMEs, insurers, academia, and the public.

1.2. Document Structure

The document begins with an outline of the project's purpose and impact maximisation strategy, followed by a detailed description of the communication and dissemination strategy, target audiences, and communication channels. Subsequent sections cover implemented activities, including branding, online presence, events, and publications. Monitoring and evaluation mechanisms are presented, alongside a summary of KPIs and performance indicators used to assess the effectiveness of these efforts. The impact KPIs (iKPIs) relevant to the overall project activities are also detailed separately in Deliverable D6.1. The report concludes with an overview of the monitoring and evaluation approach used to assess the effectiveness of these efforts, and final reflections on the outcomes achieved and the road ahead.

2. PURPOSE AND OBJECTIVES

The primary purpose of the ERMIS dissemination, communication and exploitation plan is to effectively communicate and promote the project's results in the field of cybersecurity and cyber insurance. Central to our strategy is the goal to inform and engage a broad spectrum of stakeholders, from industry experts and academic researchers to governmental bodies and potential market participants, about the capabilities and innovations developed through ERMIS.

2.1. ERMIS Impact Maximisation strategy

As already mentioned in D2.1 and subsequently supplemented in more detail, the ERMIS has devised a strategy for maximising impact based on four core pillars:

- **Pillar 1 - Mission-focused approach:** ERMIS is centred on creating a marketplace for SMEs and public organisations that provides tools, models, and services for ensuring cyber security, as well as offering cyber insurance on a service basis.
The ERMIS marketplace is designed not just as a repository of tools, but as a functional environment where SMEs and public entities can discover, adopt, and integrate cybersecurity and cyber insurance services tailored to their operational needs. Communication activities thus serve the dual function of promoting the project and facilitating user onboarding into the ecosystem.
- **Pillar 2 - Embracing openness:** ERMIS places importance on promoting open science by sharing knowledge openly and collaborating with other EU funding programs and policies.
ERMIS project actively encourages the free exchange of knowledge and leverages synergies with other EU-funded initiatives to expand its reach. ERMIS positions itself within the wider European research and innovation community, by participating in knowledge-sharing platforms, scientific publications, and joint outreach activities. This not only enhances visibility but also fosters cross-project collaboration and aligns the project with policy developments, such as the Cybersecurity Act, NIS2, and the Digital Services Act.
- **Pillar 3 - Commitment to sustainability:** ERMIS is heavily investing in research and innovation to continually integrate new knowledge and enhance existing knowledge, ensuring sustainable growth for the technological advancements to be delivered during the project.
This includes developing high-quality, reusable materials, setting up a strong digital presence, and engaging stakeholders early to foster trust and commitment. ERMIS lays the groundwork for future uptake through commercial pathways, open-source access, and integration into broader EU cybersecurity initiatives.
- **Pillar 4 - Engaging SMEs:** ERMIS aims to actively involve European SMEs in adopting cybersecurity solutions that are ready for the market, training them in the use of tool-enabled practices to enhance their cybersecurity capabilities, and incorporating cyber insurance into their business continuity and cyber resilience strategies. ERMIS follows this pillar by making dissemination activities accessible, relevant, and actionable for small businesses. This includes simplified messaging, use of local languages, hands-on events such as webinars and info days, and showcasing real-life benefits of adopting ERMIS services. Empowering SMEs through

practical guidance and exposure to cutting-edge cybersecurity solutions is central to the project's impact ambitions.

These four pillars collectively shape a coherent and strategic approach to dissemination and communication within ERMIS. By aligning project outputs with the needs and expectations of diverse stakeholders, and by embedding the values of openness, usability, and sustainability, the project ensures that its outcomes are more than just deliverables—they become catalysts for change in Europe's cybersecurity landscape.

2.2. Objectives

The primary purpose of the ERMIS dissemination, communication and exploitation plan is to effectively communicate and promote the project's results in the field of cybersecurity and cyber insurance. Central to our strategy is the goal to inform and engage a broad spectrum of stakeholders, from industry experts and academic researchers to governmental bodies and potential market participants, about the capabilities and innovations developed through ERMIS.

The objectives and the key actions implemented or designed concerning our dissemination efforts, include:

Objective 1 Awareness and Education

Description:

To raise awareness about the critical role of cybersecurity insurance in contemporary digital economies and educate potential users on the benefits and functionalities of the ERMIS Marketplace. This involves elucidating the project's scope, its innovative approach to cybersecurity risk assessment, and the advantages it offers to various stakeholders.

Key Actions:

- The ERMIS website was launched and is actively maintained, serving as the project's primary communication hub, regularly updated with project news, public deliverables, and resources.
- Three newsletters have been published to date, sharing progress updates, key milestones and partner activities.
- The ERMIS team maintains a regular social media presence on LinkedIn and Twitter/X. Posts include new items, cybersecurity awareness, participation in events and materials to engage both technical and non-technical audiences.

Objective 2 Community Building and Engagement

Description:

To foster a community of interest around the ERMIS Marketplace by conducting interactive dissemination activities that invite feedback and participation from various sectors, including technology providers, insurance companies, and regulatory entities. This will ensure that our offerings are finely tuned to market needs and are comprehensible and accessible to all relevant parties.

Key Actions:

- A dedicated workshop with major insurance companies was held during an ERMIS plenary meeting. The session focused on understanding insurer needs, exploring cyber insurance integration, and discussing ERMIS's potential to support underwriting and risk modelling processes.
- ERMIS participated in the DEP UPTAKE joint projects workshop, where the project was presented to a broader EU cybersecurity community. The session included a 15-minute presentation, a brief Q&A, and laid the groundwork for potential cross-project collaborations.

Objective 3 Integration of Stakeholder Feedback

Description:

To integrate feedback from stakeholders at various stages of the project lifecycle, such as during the development of the marketplace platform, and at key milestones of implementation. This will help refine our strategies and outputs to better serve the market's needs.

Key Actions:

- During consortium activities and external interactions, the ERMIS team has gathered valuable stakeholder feedback—particularly around the potential exploitation and practical application of the ERMIS Marketplace and its services.
- Feedback from partners and external experts has helped shape the direction of future scientific publications, particularly those addressing ERMIS's innovation potential, certification mechanisms, and its contribution to the cybersecurity insurance landscape.
- Discussions during the insurer's workshop and reviews provided insight into user expectations and perceived barriers, which are being considered in refining both the platform design and communication strategy.

Objective 4 Showcasing and Demonstrating Impact

Description:

To demonstrate the practical applications and benefits of ERMIS Marketplace through various formats and channels, including workshops, seminars, webinars, and publications. This will also include participation in both European and global events to highlight the project's innovative solutions and their impact on the cybersecurity and cyber insurance sectors.

Key Actions:

- The ERMIS consortium is preparing to showcase functional mock-ups and user interface screens during the upcoming project review in June. This will provide a visual walkthrough of the ERMIS Marketplace and its key features.
- Two scientific publications are currently under development by project partners. These papers are expected to target peer-reviewed journals and conferences in the cybersecurity and ICT domains.

Objective 5 Collaboration and Partnership

Description:

To seek and establish collaborations with other relevant EU-funded projects and international initiatives. Such partnerships will enrich ERMIS's capabilities and expand its reach and effectiveness through shared knowledge and complementary technologies.

Key Actions:

- ERMIS has taken initial steps toward collaboration by participating in the DEP UPTAKE joint projects workshop, where the project was introduced to other EU-funded initiatives, paving the way for future synergies.
- The consortium is actively monitoring opportunities for strategic collaboration with related DEP projects, particularly those focused on cybersecurity, certification, and digital trust.

Objective 6 Sustainable Exploitation**Description:**

To ensure that the results of the ERMIS project are exploited beyond the project's duration. This includes developing a clear plan for the sustainability of the marketplace, potentially through commercialisation strategies or partnerships with industrial entities.

Key Actions:

- The ERMIS consortium has initiated internal discussions on long-term exploitation scenarios, including potential commercial pathways and service models that could sustain the platform after the project's conclusion.
- Feedback received during project meetings and reviews—particularly related to market positioning and stakeholder value—has informed the early stages of the exploitation roadmap.

Through these objectives, the ERMIS project aims to not only disseminate its findings but also to achieve significant adoption and adaptation of its innovative solutions, ensuring a lasting impact on the cybersecurity and cyber insurance landscape.

Table 1. Objectives and Key Actions

Objective	Key Actions(implemented or designed)
Awareness and Education	Website, newsletters, social media
Community Building	Events, webinars, direct outreach
Stakeholder Feedback Integration	Surveys, co-design, workshops
Showcasing ERMIS Impact	Publish success stories, pilot results, videos
Collaboration and Partnerships	Liaison with EU-funded projects, standards orgs
Sustainability and Exploitation	Create reusable tools, align with market needs, build partnerships

3. COMMUNICATION AND DISSEMINATION STRATEGY

The dissemination strategy is designed to effectively engage the target groups identified in Section 3.1. The strategy leverages multiple communication channels to maximise outreach and ensure that dissemination efforts are purposeful, coordinated, and aligned with the project's overarching objectives. Rather than consisting of isolated activities, dissemination and communication actions are strategically planned to enhance visibility, foster engagement, and facilitate knowledge transfer among stakeholders. At this stage of the project (Month 18), significant progress has been made, with several deliverables and key tasks already completed. These achievements have been actively disseminated through workshops, social media platforms, and other outreach initiatives, ensuring broad awareness and engagement with both industrial and scientific communities. Moving forward, dissemination efforts will continue to evolve, incorporating feedback and optimising strategies to maximise the impact of the project's outcomes.

3.1. Target groups and Audiences

The following Table 2 provides a structured overview of the key stakeholder groups relevant to the implementation and adoption of cybersecurity assurance, certification, and cyber insurance mechanisms. For each target group, the table delineates the anticipated benefits, corresponding pathway goals, and projected impacts. This classification serves to ensure that the initiative addresses the specific needs and expectations of both primary and secondary stakeholders, while also supporting the development of evidence-based strategies that contribute to regulatory compliance, innovation, and broader societal resilience.

Table 2. Target Group Adoption of ERMIS Outcomes

Target Group	Expected Benefits	Pathway Goal	Impact
Cyber Insurance Companies (primary)	Automated or semi-automated security certification and risk assessment. Reduce the information asymmetry between insurers and clients	Testing and evaluation of insurance policies that are based on evidence-based risk assessment and analysis in real world scenarios.	A novel tool-supported framework for cyber insurance services, for personalised insurance policies, based on customer profile and risk exposure
SMEs (primary)	Availability of tools, services and processes for cyber security assurance, certification and cyber insurance	Pilots' evaluation and demonstration, Impact assessment and analysis	Strengthening innovation, risk mitigation and business continuity
Security services/tools Providers (primary)	Agile certification scheme; Optimise security Challenges; certify tools/models/processes	Self-assessing capabilities; continuous monitoring; assess effectiveness of controls	Strengthening innovation; Certification under multi-assurance levels, validated insurance policies

Target Group	Expected Benefits	Pathway Goal	Impact
Industry Associations	Regulation compliance; broad access to useful insights and tools	Pilots' evaluation and demonstration, Impact analysis	Efficient testing of end products; Mitigation action planning; Cost-effective certification methods and insurance policies
Scientific Community	Validated methods, tools, models and reference architecture	Diffuse knowledge through publications, scientific events etc.	New domain knowledge, increased capacity for new research
Open-source communities	Validation of security assurance of open-source components	Encouraging community participation and infusion of cyber security in open-source solutions	Enhanced inclusion of opensource solutions in cyber insurance policies and improvement of their security posture
Conformity Assessment Bodies	Certification models that incorporate risk management and cyber insurance of cyber systems	Demonstration of validated and harmonised certification services and models that combine certification, risk management and cyber insurance	New model driven certification framework for testing and monitoring different types of evidence.
Policy Makers (primary)	Better insights into policy deficiencies and gaps; availability of conformity- related information	Report actionable knowledge	Definition of future research and EU innovation directions
Consumer Associations & General Public	Secured and certified services, tools and processes	Increase general awareness through communication strategy	Increased awareness about security assurance, certification and cyber insurance value in consumed services

3.2. Communication Channels

A set of communication channels has been established to disseminate the ERMIS project's message and important information around it in order to achieve an effective communication and ensure that key findings and results reach the stakeholders and the wider community. These channels include traditional media, such as press releases, newsletters and promotional material, like flyers/brochures and e-brochures, which are designed to inform and raise awareness among the target audiences. In addition, online publications and articles provide in-depth information on project developments and findings. Digital marketing platforms, including the project website and social media, further expand the project's visibility and promote ongoing interaction with the community. Finally, events and workshops offer opportunities for direct engagement, knowledge sharing and collaboration with stakeholders. A detailed analysis of each communication channel and its implementation strategy is presented in the following sections.

4. COMMUNICATION AND DISSEMINATION ACTIVITIES

4.1. ERMIS Brand guide

4.1.1. ERMIS LOGO

The final version of the ERMIS logo that all partners agreed to is shown below.



4.1.2. ERMIS COLOURS

The final dominant colour codes for the ERMIS project depending on the background that all partners agreed to, are shown below.



#5D6771



#0F3877



#A7C4E7



#FFFFFF

4.1.3. DEVELOPMENT OF PROJECT TEMPLATES

To ensure consistency and clarity with the project standards, a comprehensive set of templates has been developed in alignment with the operational and reporting needs of the ERMIS project. These templates serve as standardised tools to support effective communication, documentation and coordination between all project partners. Specifically, templates have been designed for official project deliverables, PowerPoint presentations, financial reports, meeting agendas, and minutes of weekly coordination meetings. The adoption of these templates facilitates streamlined collaboration, improves the quality and uniformity of outputs and supports the overall management and traceability of project activities.

4.2. The funding information

In accordance with the provisions outlined in the Grant Agreement, all communication activities related to the ERMIS project, including electronic communications and social media engagements, as well as any infrastructure, equipment, or significant outcomes financed by the grant, must adhere to the following requirements:

Table 3. Funding Requirements

A) prominently feature the EU and ECCC emblem	 Co-funded by the European Union 
B) contain the following statement	<p>Website: This project has received funding from the European Union's Horizon Europe Research and Innovation program under Grant Agreement No 101128013. The website reflects only the view of the author(s) and the Commission is not responsible for any use that may be made of the information it contains.</p> <p>Newsletter(s):</p> <ul style="list-style-type: none"> Short version (up to 2 pages): This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101128013. Rich version: Funded by the European Union (Grant Agreement No 101128013, ERMIS Project). The views and opinions expressed are however solely those of the author(s) and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. <p>Promotional videos: This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101128013.</p> <p>For infrastructure, equipment, and major results: This [infrastructure][equipment][type of result] is a component of ERMIS project that has been sponsored by the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101128013.</p>

4.3. ERMIS Website

The official ERMIS project website (<https://dep-ermis.eu>) serves as a central communication and dissemination platform, offering comprehensive and up-to-date information on all aspects of the initiative. It provides an overview of the project's vision, objectives, and strategic goals, while also highlighting its relevance within the broader context

of cybersecurity assurance, certification, and cyber insurance under the Digital Europe Programme. In addition to core project information, the website features regularly updated news items and press releases that communicate the latest developments, milestones, and outcomes, including plenary meetings, workshops, and other key events.

To enhance stakeholder engagement and transparency, the website also hosts newsletters and e-brochures that provide in-depth coverage of project activities, achievements, and opportunities for collaboration. A dedicated section presents detailed information on project deliverables, ensuring public access to key outputs and results. Furthermore, the website includes a comprehensive description of the project consortium, offering insights into the roles and expertise of each participating organisation. Collectively, these components support the ERMIS project's objectives for visibility, outreach, and impact across the European cybersecurity ecosystem.

A detailed analysis of each workshop, brochures, newsletters and events organised by ERMIS is presented in the following sections.



Figure 1. ERMIS "Home Screen Upper top"

Our Goals

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.
- Improve the security of open-source solutions.

[Learn About Our Objectives](#)



Industry Challenges and Market Needs



News and Updates

Stay informed and connected by subscribing to our updates

[Subscribe](#)



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre

Copyright © 2025 DEP - ERMIS | Powered by ERMIS. All rights reserved



Figure 2. ERMIS "Home Screen Bottom"

4.4. Social Media

ERMIS strategically utilises social media to amplify scientific and political awareness, ensuring broad outreach and engagement. To maximise impact, the project employs four primary platforms:

4.4.1. LINKEDIN

The LinkedIn page (DEP-ERMIS), managed by ZELUS, provides a more detailed space for professional engagement. In this platform, ERMIS shares in-depth insights into research developments, major findings, and collaborations. As the

project advances, LinkedIn activity expands, featuring more frequent updates on scientific breakthroughs, participation in key events, and consortium-organised initiatives. The platform fosters discussions, strengthens professional connections, and enhances visibility among industry stakeholders, funding bodies, and researchers.

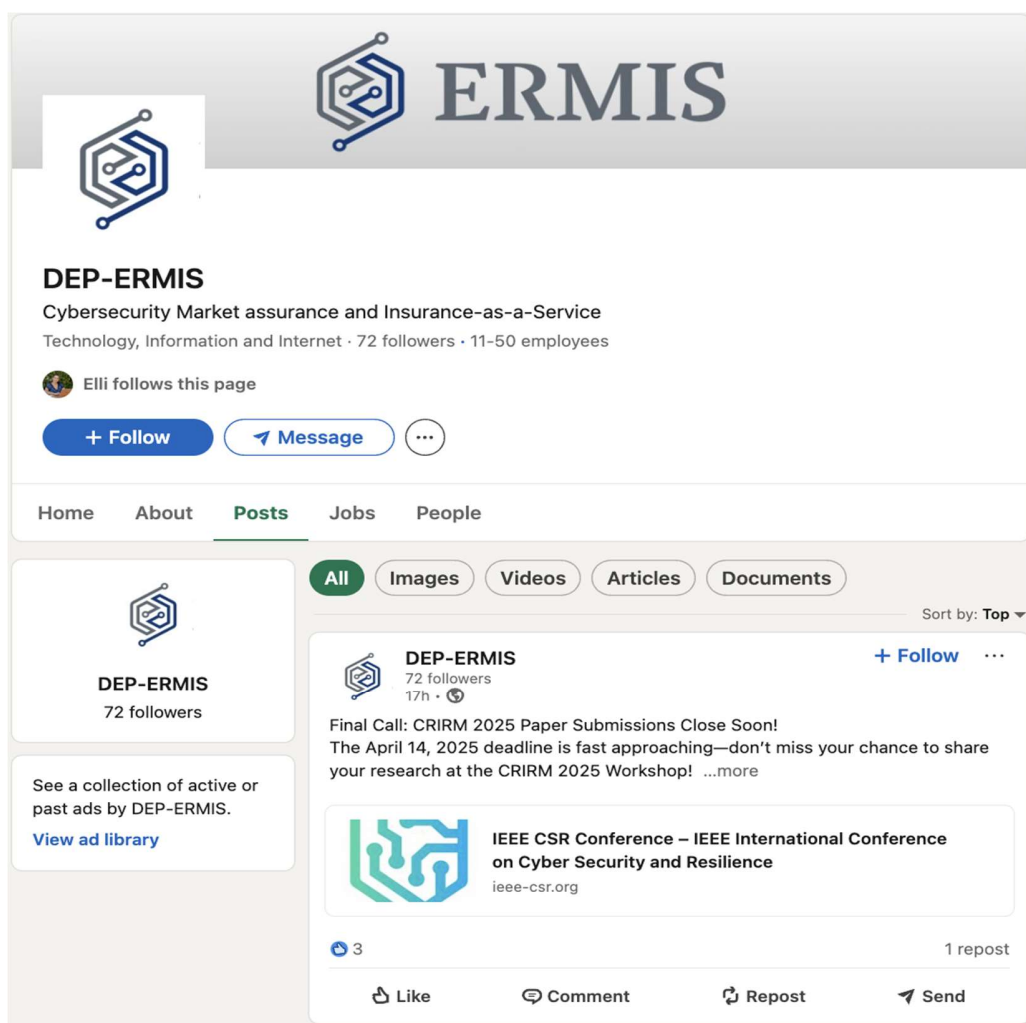


Figure 3. ERMIS LinkedIn account

4.4.2. TWITTER/X

The official X account (@DEP_ERMIS), also managed by ZELUS, serves as a rapid communication channel for sharing technical achievements, project milestones, and participation in industry events such as conferences and exhibitions. Consortium-led initiatives, publications, and collaborations are also highlighted. As ERMIS progresses, the frequency of updates increases, reflecting ongoing advancements and ensuring continuous engagement with the research

community, policymakers, and industry leaders. Project partners play an active role in contributing content to maintain a steady stream of relevant information, often linking to additional resources for further insights.



Figure 4. ERMIS Twitter/X account

4.4.3. YOUTUBE

The ERMIS YouTube channel was created early in the project but has not yet been utilised since its aim is to accommodate for sharing marketplace-related infographic and guidance videos, including technical demonstrations. As the project implementation advances, video content will play a crucial role in making marketplace usage concepts more accessible, engaging a broader audience, and fostering interaction with stakeholders.

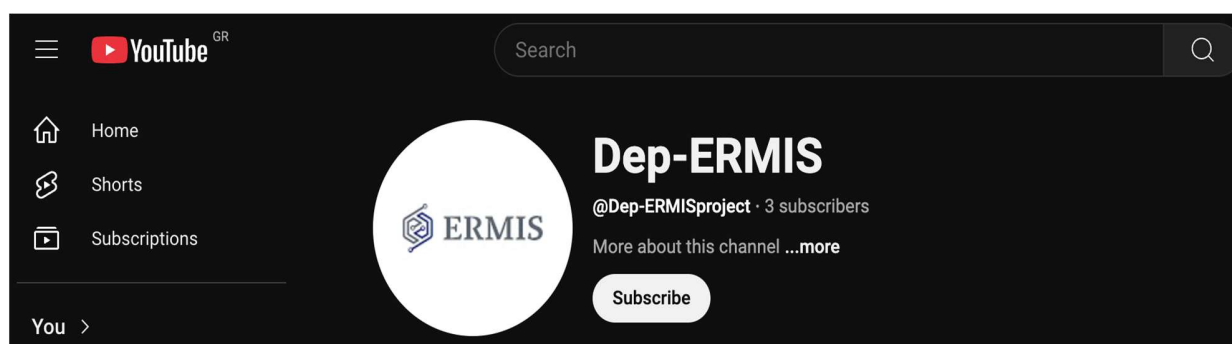


Figure 5. ERMIS YouTube account

4.4.4. RESEARCH GATE / ZENODO

The ERMIS Zenodo community was established to support the dissemination of project results. It will host publications, reports, datasets, and other relevant outputs throughout the project's lifecycle. The first report, entitled "Cyber Insurance Application Guide" has already been published, marking the beginning of our effort to make ERMIS outcomes widely accessible to the research and innovation community. Expected publications and public deliverables will be also uploaded in the Zenodo account.

CYBER INSURANCE APPLICATION GUIDE

Karavias Underwriting Agency (Editor)

Cyber threats continue to evolve in both complexity and impact, affecting organizations of all sizes and sectors. To effectively underwrite cyber risk, insurers require a comprehensive understanding of the applicants' business structure, data handling practices, security controls, historical incidents, and preparedness for potential cyber events.

The information requested in the Cyber Insurance Application form is essential for insurers to accurately assess the applicant's cyber risk exposure, determine the appropriate scope of coverage and ensure the policy is tailored to the specific operational, technical, and regulatory context of an organization.

Each section of the application form is designed to capture relevant and actionable information that supports a thorough risk assessment and promotes transparency between the insured and the insurer. The ultimate goal is to clarify the importance of each data point, ensure understanding for the applicant, and demonstrate how this information contributes to fair and accurate underwriting decisions.

This document provides a justification analysis, explaining the rationale behind each section of the Cyber Insurance Application Form.

Files



Figure 6. ERMIS Zenodo first publication

4.5. Communication Material

4.5.1. E-BROCHURE

The brochures serve as a concise, yet comprehensive communication tool designed to highlight the core objectives, strategic components, and key stakeholders involved in the initiative. Developed for dissemination to a broad audience, including policy makers, industry representatives, SMEs, and the research community. Visually supported by a graphical representation of the ERMIS framework, the brochure illustrates six interrelated focus areas of the cybersecurity assurance and insurance marketplace: Dynamic Security Certification, Risk-aware Cyber Insurance, Improvement of Cybersecurity Capabilities, Training and Cyber Range, Deployment of Assurance Tools, and Evidence-based Risk Management. The brochure also introduces the project consortium, showcasing the collaborative nature of the initiative. As a key communication asset, the brochure is instrumental in raising awareness, enhancing stakeholder understanding, and promoting the ERMIS vision throughout the European cybersecurity landscape.



ERMIS

Co-funded by the European Union

ECCC

Cybersecurity Assurance & Insurance Marketplace

The ERMIS marketplace platform will support the adoption and deployment of market-ready innovative cybersecurity solutions.

OBJECTIVES

- Design, implement and deliver a TRL-7 and highly usable cybersecurity, certification and cyber insurance management marketplace
- Deliver market-ready tools for increasing the resilience and preparedness of SMEs against cyber threats
- Deliver market-ready tools, processes and models for the agile and verifiable certification of cyber systems, ensuring the conformity assessment and validation
- Deliver market-ready tools, processes and models for the agile and verifiable certification of cyber systems, ensuring the conformity assessment and validation
- Validate the ERMIS offerings in real world environments and business cases for improving cybersecurity assurance capabilities in the EU and enhancing cyber insurance management
- Raise awareness on the innovative ERMIS results to business, research, academic, and open-source communities in the EU and empower their skills in addressing ongoing cybersecurity challenges.

ERMIS Cybersecurity Assurance & Insurance Marketplace

Dynamic Security Certification

Risk-aware Cyber Insurance

Improvement of Cybersecurity Capabilities

Training and Cyber Range

Deployment Cybersecurity Assurance Tools

Evidence-based Risk Management

PROJECT TEAM

Zelus **Sphynx** **Insuretics** **Nodalpoint** **karavias** **underwriting agency** **ΕΛΛΗΝΙΚΗ ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΕΙΑ**

The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre

<https://dep-ermis.eu/> info@dep-ermis.eu [in DEP-ERMIS](https://www.linkedin.com/company/dep-ermis) [#DEP_ERMIS](https://twitter.com/DEP_ERMIS)

Figure 7. ERMIS e-Brochure

4.5.2. PROJECT PRESENTATION

The ERMIS project is formally presented through a presentation which is delivered by the project coordinator. So far it was presented during the UPTAKE event on September 19th, 2024, the first ERMIS Info Day, held on December 13th, 2024 in Cyprus as well as the Insurance companies workshop organised in Athens on February 18th, 2025. This presentation provided an in-depth overview of the project, outlining its primary objectives, its ambitions and the strategic goals. In addition to these foundational elements, the presentation offered a thorough analysis of the project's overarching vision, proposed architecture, implementation framework, and detailed work plan. It also addressed the anticipated outcomes and the role of the ERMIS platform of the cybersecurity insurance and assurance services marketplace (see Annex 2 for details).

4.5.3. PROJECT BANNER

The ERMIS project's official promotional banner, shown below, is intended to graphically represent the project's primary vision and strategic goals. The banner clearly reflects the initiative's primary goal: to provide cybersecurity assurance and insurance as a service through the creation and deployment of an innovative, market-ready marketplace platform. The banner highlights six important subject elements that underpin the project: dynamic security certification, risk-aware cyber insurance, improvement of cybersecurity capabilities, deployment of cybersecurity assurance tools, training and cyber range, and evidence-based risk management. These pillars demonstrate ERMIS' commitment to integrate innovative technologies, services, and processes to improve cybersecurity resilience throughout Europe. The banner, with its obvious visuals and brief form wording, is an important outreach asset for use at conferences, seminars, other dissemination events, emphasising the project's identity and aims.



ERMIS

Cybersecurity Assurance & Insurance Marketplace

THE ERMIS MARKETPLACE PLATFORM WILL SUPPORT THE ADOPTION AND DEPLOYMENT OF MARKET-READY INNOVATIVE CYBERSECURITY SOLUTIONS.

OUR GOALS

ERMIS project aims to deliver cyber security assurance and insurance as-a-service, by integrating mechanisms, services, and tools in an innovative marketplace platform.

- Dynamic Security Certification
- Risk-aware Cyber Insurance
- Improvement of Cybersecurity Capabilities
- Deployment Cybersecurity Assurance Tools
- Training and Cyber Range
- Evidence - based Risk Management

Co-funded by the European Union

ECCC

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101128013

Project Team

Zelus, Epimix Hellas, Insurectics, karavias, Nodalpoint, CAIRNOS UNIVERSITY

Figure 8. ERMIS Zenodo first publication

4.6. Newsletters and Press Releases

As part of the project's Dissemination and Communication strategy, three newsletters have been released to date, providing stakeholders with key insights into ERMIS developments, industry trends, and project milestones. These newsletters serve as a vital communication tool, ensuring ongoing engagement with the project's audience.

- Issue #1 – April 2024: The inaugural edition introduced the ERMIS project, outlining its objectives, scope, and anticipated impact. It provided readers with an insightful overview of the initiative and set the foundation for future updates.



Page 1



Page 2

Figure 9. Newsletter Issue #1

- Issue #2 – November 2024: This edition focused on key industry topics, including static and dynamic cyber insurance policies, emerging trends in cyber solutions and security services, and an overview of the NIS2 Directive. Additionally, it featured an announcement regarding the first ERMIS plenary meeting, held in Cyprus.



ERMIS

Newsletter

November 2024 - Issue No2

In this Issue

The NIS2 Directive

Cyber Solutions and Security Services Trends

Static and dynamic cyber insurance policies

Plenary Meetings

The NIS 2 Directive enters our lives

It is several years since October has been pronounced as the chosen month dedicated to Cyber Security. This year, however, there is a solid cause and a distinguished circumstance for this: October the 18th was the set day for Member States to transpose the Directive 2022/2555 [Directive on measures for high common level of cybersecurity across the Union - NIS2] into their national law and apply necessary measures to be compliant to the provisioned cybersecurity rules, including supervisory and enforcement measures. In recent months, the entire cyber security ecosystem is engaged in an unprecedented race to ensure timely and effective preparedness. This article attempts a brief overview of the upcoming landscape.

As for the European Acts and laws, the NIS2 is the most iconic one. Its main objective is to achieve a high common level of cybersecurity across the European Union. To ensure this, the NIS2 is based on three pillars: Firstly, Member States have to deploy national capabilities. This includes the development of a national cyber security strategy, the appointment of national competent authorities to oversee its implementation along with a package of more comprehensive monitoring measures and administrative fines in case of non-compliance. A national cyber security incident response team to assist entities with incident response, the implementation of a national vulnerability disclosure policy and the deployment of a cyber crisis management framework.

Secondly, the NIS2 highlights international cooperation using well established or emerging schemes and mechanisms such as the NIS Cooperation Group, the CISRS Network, the Cyber Crisis Liaison Organization Network, the shared EU Vulnerability

Database, a cross-border entities' Registry and the annual EU cybersecurity status Report. The abovementioned collaboration covers mainly the areas of strategic information exchange and cross-border incident response on both technical and operational level. Third, the entities within the scope of NIS2 must ensure responsibility of their management bodies when it comes to cybersecurity practices and law compliance. Management bodies approve the adequacy of the cybersecurity risk-management measures taken by them, supervise their implementation and subsequently are accountable for non-compliance. In this context, they follow relevant trainings and offer their employees trainings on a regular basis.

Moreover, the compliance of specific requirements includes detailed risk-management measures, such as the accomplishment of cyber risk assessments, the mitigation of risks through appropriate security measures and the maintenance of specific time constraints for incident reporting. Specifically, in case of a significant cyber incident, the NIS2 provides the entity with twenty-four hours to issue an early warning, seventy-two hours for the incident notification and one month for the final report.

There is a wide feeling among the cybersecurity stakeholders that in this case the European Union has done well, especially considering the multidisciplinary and multilevel nature of cybersecurity and the need for organized posture in each one of these levels. It remains to be seen how the new member of European legislation will take its first steps...

By Georgios Kittes, MDG

3 Pillars of NIS2 DIRECTIVE

1. Member State Capabilities

2. Risk Management

3. Cooperation and Info Exchange



On Sept 18th, the Ministry of Digital Governance presented the NIS2 Directive to our consortium partners! Below are some key insights on new cybersecurity regulations and the future of digital security in the EU were shared.











Cyber Solutions and Security Services Trends

Cyber solutions & Security Services Revenue



Source: Statista Market Insights

The revenue from cyber solutions and security services has been steadily increasing and is projected to grow significantly in the coming years, as reflected in the recent Statista Market Insights, Jun24. In 2016, the combined revenue of these services was \$483.2 billion, with significant growth in both cyber solutions and security services over the years. By 2024, the total revenue is expected to reach \$202.99 billion, with projections showing further increases to \$255.70 billion by 2028 and \$271.90 billion by 2030. This growth highlights the escalating demand for cybersecurity services, likely driven by the rise in global cyber threats and the increased focus on digital resilience in response to geopolitical factors. As cyber threats continue to evolve, the market for cyber solutions and security services is set to expand, underscoring the critical role these services play in safeguarding digital infrastructures worldwide.

By Mary Tsasoulis, INS

(Data source: Statista Market Insights, Cybersecurity: market data & analysis, Jun24)

Static and dynamic cyber insurance policies

As the cyber insurance market continues to mature, collaboration between insurers, technology providers and policymakers will be vital. The rapid pace of technological change means that static annual policy renewals may become obsolete and be replaced by innovative dynamic, data-driven risk transfer insurance solutions that adapt in real-time to a changing threat landscape. ERMIS's innovation is about a market platform that offers cybersecurity assurance and insurance as a service.

By Dimitra Smyrli, INS

1st Plenary Meeting

The 1st plenary meeting took place in Nicosia, Cyprus on September 26-27th, 2024. We brought together all participating companies to review progress and align key project goals. We had discussions centred on the progress of all Work Packages (WPs) and planning the next steps.





http://dep-ermis.eu/











http://dep-ermis.eu/











http://dep-ermis.eu/











http://dep-ermis.eu/







Figure 10. Newsletter Issue #2

Issue #3 – March 2025: The latest issue highlighted significant project activities, including insights from the Cyber Insurance Workshop and discussions on cyber insurance from an SME client's perspective. It also covered regulatory updates, such as the Digital Operational Resilience Act (DORA), and provided a recap of the second ERMIS plenary meeting in Athens.



Figure 11. Newsletter Issue #3

- The ERMIS project has actively shared updates through its 'News' section on the website, highlighting major milestones and stakeholder engagement. These include details on its kick-off and two plenary meetings in Athens and Nicosia, its first Info Day in Cyprus as well as a training workshop focused on the NIS2 Directive that was organised for the partners. Additionally, press releases underscore institutional support from the Greek Ministry of Digital Governance and the National Cybersecurity Authority, reinforcing ERMIS's alignment with national and EU cybersecurity priorities.

4.7. Workshops and Events

Workshops and events play a crucial role in the ERMIS project's Dissemination and Communication strategy, providing key stakeholders with opportunities to engage, exchange knowledge, and gain insights into the latest advancements in cyber insurance, cybersecurity policies, and digital resilience. These activities support collaboration between industry experts, policymakers, researchers, and SMEs, ensuring that the project's outcomes are effectively communicated and widely adopted. So far, the following have been carried out:

The project officially launches with its kick-off meeting on 21st of November 2023 in Athens, Greece, organised by Zelus. With the official start of this innovative initiative, project objectives, milestones, detailed planning for each work package and key highlights of the meeting discussed included a detailed introduction to the project's objectives,

expected outcomes, and overall timeline, each work package discussion, examine and presenting with partners their plans and timelines and the networking and collaboration, making an environment that will be crucial for the project's success.

On 18th of September 2024 the Director for Strategic Cybersecurity Planning at the National Cybersecurity Authority of the Ministry of Digital Governance, Mr. Ioannis Alexakis, delivered an exclusive presentation on the NIS2 Directive to project partners. This crucial briefing highlighted the upcoming changes in cybersecurity regulations, emphasising the need for enhanced digital resilience.


The first Plenary Meeting took place in Nicosia, Cyprus on 26th and 27th September 2024 hosted by Insuretics. The meeting was held in a hybrid format, bringing together project partners both in person and remotely. This highly constructive session provided an opportunity to review all work packages, assess project progress, and strategically plan the next steps. A key highlight was the participation of our Project Officer (PO), Alina Taralunga, who joined remotely to provide valuable support and deliver an insightful presentation on the Digital Europe Programme framework, further aligning ERMIS with the broader EU digital strategy.


The first Info Day took place in Nicosia, Cyprus on 13th of December 2024 hosted by Insuretics. It was a hybrid event that brought together more than 25 stakeholders and cyber security and cyber insurance experts both on-site and online to explore the exciting vision and goals of the project and attendees learned about the project's core mission, its impact, and the roadmap ahead.

The second Plenary Meeting took place in Athens, Greece on 17th and 18th of February 2025 hosted by Karavias Underwriting agency. It served as a forum to assess project developments; review completed deliverables and refine upcoming dissemination strategies. Key discussions included regulatory updates such as the Digital Operational Resilience Act (DORA), advancements in cyber insurance policies, and industry best practices for enhancing cybersecurity frameworks. It also allowed partners to align key milestones and next steps in developing a robust cybersecurity assurance and insurance marketplace.

The second plenary meeting was followed by a Workshop on Cyber Insurance and Cybersecurity on the 18th of February 2025. It specialised on critical topics related to cyber insurance, including risk assessment methodologies, SME perspectives on cyber insurance adoption, and the latest trends in security solutions. The session featured expert presentations and interactive discussions, fostering valuable insights among attendees.


ERMIS will continue to organise workshops and events to engage stakeholders, share research findings and promote the adoption of cyber insurance solutions in the industry. By actively hosting and participating in these events, ERMIS promotes dialogue and collaboration in the cyber insurance ecosystem, ensuring that its knowledge contributes to policy development, industry standards and practical applications. Details of upcoming events will be announced via the ERMIS website, social media channels and project newsletters.





ECCC
EUROPEAN CYBERSECURITY
COMETENCE CENTRE

Info Day - 13th December 2024



ERMIS

Cybersecurity market assurance and insurance-as-a-service

Digital Europe Programme (DIGITAL)
Call: DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS

Consortium:
Sphynx Hellas Single Member P.C. (SPH)
Insurectics Limited (INSU)
ZELUS IRE (ZELUS)
Karavias Mesites Asfaltheon kai Symvouloi Asfaltheon (KAR)
NodalPoint Systems Ltd (NDP)
Ministry of Digital Governance (MDG)

Project No: 101128013
Type: JU SME Support Actions
Start date: 01 Nov. 2023
Duration: 36 months
Website: <https://dep-ermis.eu/>
Lead Partner: ZELUS

101128013 - ERMIS - DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS

Agenda

Meeting From / To	13 th December, 14:00-15:00 (CY Time)
Meeting type (Location)	<p>INFO DAY Host Partner: Insurectics (INSU) Location: <i>The classic Hotel</i> Meeting Room: Van Gong Hall</p>
Remote attendance links	Meeting Link

Time	Topic	Lead
14:00 – 14:05	Welcome to ERMIS Info Day!	INSU
14:05 – 14:40	Presentation of ERMIS Project by Dr. Emmanouil Vergis	ZELUS
14:40 – 15:00	Q&A and Open Discussion	

ERMIS - Cybersecurity market assurance and insurance-as-a-service

Figure 12. Agenda of the Workshop on Cyber Insurance and Cybersecurity

4.8. Journal Publications, Scientific Papers and Conferences

As part of its dissemination and scientific outreach strategy, ERMIS significantly emphasised contributing to the broader cybersecurity research community through high-quality publications and active participation in scientific events. The project's planned actions in this area include the following:

- **Publishing Peer-Reviewed Articles:** ERMIS aims to publish findings, methodologies, and evaluation results in reputable journals covering cybersecurity, resilience engineering, and critical infrastructure protection. These publications would reflect both the theoretical foundations and practical outcomes of the project, ensuring wide academic impact. At the time of writing this deliverable, ERMIS plans to submit a number of articles in (a) IEEE CRIRM¹ and (b) the Special Issue on Cyber Range, Incident Response, and Cyber Insurance in Critical Infrastructure²
- **Conference and Workshop Participation:** Members of the ERMIS team plan to present at leading national and international conferences and workshops. Such engagements not only increase visibility but also foster collaborations and knowledge exchange.

¹ <https://www.ieee-csr.org/crirm/>

² <https://link.springer.com/collections/dhcaiadihg>

- **Joint Scientific Contributions:** The consortium encouraged joint publications among partners, bringing together academic, industry, and policy perspectives. This multidisciplinary approach strengthens the quality of the scientific output and aligns with ERMIS's goal of integrating technical and organisational resilience strategies.
- **Open Access and Repository Uploads:** To promote transparency and wider accessibility, ERMIS is committed to making scientific outputs available in open-access repositories whenever possible, by Horizon Europe guidelines and FAIR data principles.

Through these actions, ERMIS contributes meaningfully to the advancement of knowledge in the field of cyber resilience while also demonstrating the practical applicability and societal relevance of its work.

4.9. Communication Material - Dissemination Communication Exploitation (DCE) table

The Dissemination, Communication, and Exploitation (DCE) activities are an integral part of a dedicated horizontal Work Package (WP2), coordinated by Insuretics and overseen by the Dissemination, Communication, and Exploitation Committee (DC), which includes experts from each project partner. Insuretics oversees communication and dissemination efforts, ensuring that content and material is finalised and distributed effectively across various channels. This includes publishing updates on the project's website and promoting key developments through social media, in collaboration with designated partners.

5. MONITORING AND EVALUATION OF COMMUNICATION AND DISSEMINATION ACTIVITIES

5.1. Monitoring

The continuous monitoring and reporting of communication and dissemination activities in ERMIS project is intended not only to measure the effectiveness of these activities, but also to increase their relevance and encourage partners to be continuously involved and actively engaged in the project's objectives. To monitor dissemination and communication activities, a spreadsheet has been created in the ERMIS Google drive, which is accessible to all partners. This shared document provides a structured and transparent system for capturing all dissemination and communication efforts. It includes a tracker file to record all project actions and all key performance indicators and allows partners to report activities such as event participation, journal publications, social media engagement and content creation. This form allows partners to easily submit individual dissemination activities, which are then compiled into the tracking system. Furthermore, the ERMIS consortium has organised weekly meetings to present and update the partners on the progress share updates, encourage contributions and to ensure that all partners remain informed and actively engaged in the project's outreach goals.

An online form has been introduced to easily gather input on Dissemination and Communication activities which facilitate the process and collects information in a central repository. The input will be collected in the ERMIS DCE form by Insuretics and the summary is one of the main tools used to monitor the DCE activities and will be used to update the platform (see Annex for details).

5.2. Reporting

CDEB Objective 1 | Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators.

Measure 1.1: The consortium will set the **ERMIS impact tracker** to monitor the effectiveness of the communication strategy implemented using the following dissemination instruments: Project website, social media, video material, scientific communities and research networks.

KPI	Target Value	Achieved during M1-M18
Visits annually (average)	≥ 500	1816
Downloads (deliverables, results & materials)	≥100 until the end of the project	55
Push announcements	≥10 until the end of the project	N/A
New followers in Twitter / LinkedIn	>5 monthly	95 ³

³ There are 22 followers in Twitter and 73 in LinkedIn as of April 30, 2025

Re-tweets	≥20 per year	81
Posts	≥30 per year	42
Project accounts in ResearchGate*, LinkedIn	2	2
Target group:	SMEs, the general public, cyber security and insurance Industry, academics and research organisations	

*The ResearchGate has been replaced by the equivalent platform Zenodo.

CDEB Objective 1 Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators		
Measure 1.2: A regular (bi-monthly) e-newsletter will be sent to ensure that core information on project progress, achievements and next steps are shared. The newsletter will seek to strengthen networking and loyalty of interested stakeholders		
KPI	Target Value	Achieved during M1-M18
e-Newsletters with technical activities by the end of the project	≥8	3
e-Newsletter receivers	≥1500	36
Target group:	SMEs, the general public, cyber security and insurance Industry, academics and research organisations	

CDEB Objective 1 Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators.		
Measure 1.3: A communications starter pack will be produced early on M2 (T2.1) for partners to ensure consistency in developing a project brand. This will also include a preliminary list of external events at which partners are representing the project.		
KPI	Target Value	Achieved during M1-M18
Full guide about CDEB strategy, measures and planned actions distributed to all project partners.	≥1	1 ⁴

⁴ Deliverable 2.1 published in M6

Target group:

Project Partners

CDEB Objective 1 Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators.

Measure 1.4: A regular update of the communication, dissemination and exploitation plan with lessons learnt will take place every year M12/M24/M36 (T2.1). This includes breakdown of target stakeholder groups, a timeline of key EU/international related events, consultations and policy milestones over the lifetime of the project, with a clear strategy for planned ways to engage with these.

KPI	Target Value	Achieved during M1-M18
Versions of the CDEB plan	≥3	2 ⁵
Target group:	Project Partners	

CDEB Objective 1 Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators.

Measure 1.5: Early contact with key work groups (e.g. consortia from similarly themed projects, cyber security initiatives, EC institutions, ENISA) will be incrementally made to discuss collaboration opportunities through scoping ways to foster the project impacts.

KPI	Target Value	Achieved during M1-M18
Similarly themed projects and initiatives identified	≥10	6 ⁶
Jointly organised workshops	>5	2
Target group:	Project Partners, research organisations	

⁵ Deliverable 2.1(M6) and Deliverable 2.2 (M18)

⁶ SYNAPSE, SecAwareness Truss, NERO, CYSSDE, Cybersuite & Cyberunity

CDEB Objective 1 | Raise national and international awareness of the project and its objectives and the ways in which ERMIS delivers value to end-users and European SMEs. Drive demand among SMEs, service providers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators.

Measure 1.6: The ERMIS partners will carefully select publication venues based on their scientific excellence and impact privileging where possible open access publishing. Indicative journals and conferences and that will be targeted include: Journal Cybersecurity (Springer), Journal of Cybersecurity (Oxford Academic), International Journal of Critical Infrastructure Protection (Elsevier), Journal Computers & Security (Elsevier), Transactions on Artificial Intelligence (IEEE), Journal of Machine Learning (Springer), Journal of Machine Learning Research (Microtome), Journal on Data Quality (ACM), Journal of Surveillance, Security and Safety, International Security, International Journal of Smart Security Technologies, Cyber and Space Security conference, etc.

KPI	Target Value	Achieved during M1-M18
Publications in international referred publications	≥6	N/A
Publications in international magazines	≥6	N/A
Conference/ scientific events/ industrial for presentations	≥10	N/A
Target group:	Project Partners, research organisations	

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

Measure 2.1: ERMIS aims to find mechanisms for better feed-in from the project to the EU priorities on digital skills and especially in cybersecurity capabilities, skills and cyber security services uptake. This will be achieved through initiating scoping activities with key working groups to open up discussion around some of the aspects (e.g., cyber insurance, digital Hubs, cybersecurity certification) being funded by the European Commission in order to ensure that a variety of voices are present. These discussions aim to provide priority recommendations for specific topics such as: interoperability, sharing cyber exercises, certification schemes, homogenizing the curricula, development of green, energy and cost-efficient services.

KPI	Target Value	Achieved during M1-M18
Downloads of high-quality electronic brochures with the technical approach and activities	≥1000	24
New discussions in LinkedIn	≥50	N/A
Target group:	SMEs, the general public, cyber security and insurance Industry, academics and research organisations	

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

Measure 2.2: A website with a dedicated private partner space will host key information produced by the project from M2, including reports, 5-min videos created for You-Tube, infographics, webinar downloads, as well as summaries of all activities and ways to get involved.

KPI	Target Value	Achieved during M1-M18
Downloads monthly on average	≥20	N/A
Video demonstrators of ERMIS	≥4	N/A
Views of 5-min videos in You-Tube by the end of the project	≥10	N/A
Target group:	Industry actors, research and academic community and the general public.	

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

Measure 2.3: A series of in person-events will be organised including: three (3) open INFO days (M12, M21, M33), a technology showcase event in M27, workshops, virtual participation tools, e.g. live streaming, and a pan-European (final event) conference in M36 to present results of the project.

KPI	Target Value	Achieved during M1-M18
Events (up to 25 participants)	≥5	1
Events (25-100 participants) organised by the end of the project	≥3	2
% of Participants in each event attracted and registered as contacts	≥40%	N/A
Target group:	Industry, research and academic community, ICT and domain experts	

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

Measure 2.4: Public consultation and policy events involving policy makers and relevant working groups (identified through e.g. policy fellowship schemes) will be closely monitored and results will be presented in open national and international networking events in order to boost reciprocal relationships between students, academics, sectoral specialists, researchers, industry and policy makers (e.g. Ministries of Education) focusing on crucial advance trainings of digital skills. The aim is to let them know the progress accomplished in ERMIS and influence them to capitalise on the project results and on the demonstrator outcomes and best practices identified.

KPI	Target Value	Achieved during M1-M18
Hard copies distributed in ≥5 events	≥150	N/A
Engagement of policy making bodies	≥7	2 ⁷
Target group:	Policy makers Industry, research and academic community	

CDEB Objective 3 | Work to deliver and monitor project impacts as related to exploitation of outputs.

Measure 3.1: Presentation of the results to engage different stakeholders for exploitation of the outputs through project visits to education and industrial open days and networking events, organisation of workshops, participation to selected EU Annual Meetings, conferences and exhibitions (e.g., International Cyber Expo, Undersea Defense Technology event, Border Security Expo, Eurosatory). Engagement will be particularly strengthened by suggestions coming from the ERMIS partners, especially the pilot partners, as well as the technical partners after analysing the relevance of their contact network members to the project and ad-hoc identification processes.

KPI	Target Value	Achieved during M1-M18
Participation in small and large-scale events by the end of the project	≥ 10	1 ⁸
Events organised with ≥100 attendees	≥ 2	1 ⁹
Participants engaged for further exploitation	≥ 20%	20% ¹⁰

⁷ Enisa and DSA Cyprus

⁸ UPTAKE event

⁹ IEEE

¹⁰ We had meetings with other projects for further exploitation from UPTAKE event with 2 projects (CYSSDE & NERO)

Target group:

Enterprises in security assurance, certification and cyber insurance domains as well as ICT specialist and security systems providers

CDEB Objective 3 | Work to deliver and monitor project impacts as related to exploitation of outputs.

Measure 3.2: Internal Consortium monthly emails will be sent to inform about project progress, upcoming events, round-table discussions and dissemination and exploitation opportunities.

KPI	Target Value	Achieved during M1-M18
Emails with rich information on project progress and DE events & opportunities	≥15	18
Target group:	Project partners	

CDEB Objective 3 | Work to deliver and monitor project impacts as related to exploitation of outputs.

Measure 3.3: Quarterly reports will be compiled to monitor the results and update the CDEB plan. These will include a set of KPIs that will be regularly updated in order to quantitatively monitor the expected impact of the proposed measures. These KPIs will be also leveraged to evaluate marketing effectiveness, validate market potential and key insights.

KPI	Target Value	Achieved during M1-M18
Reports published with CDEB KPIs that are continuously updated.	6	3
Target group:	Project partners	

CDEB Objective 4 | Accelerate business growth through direct and indirect integration of the project's benefits.

Measure 4.1: Training and awareness workshops relevant to the project's pilot results and achievements will be organised internally in each partner organisation to build staff capacity. Training Need Assessment will be conducted and capacity development will be assessed at the end of the workshop.

KPI	Target Value	Achieved during M1-M18
-----	--------------	------------------------

Internal(partners) trainees for becoming familiar with the ERMIS training tools and program		≥20	N/A
Target group:	Project partners		

CDEB Objective 4 | Accelerate business growth through direct and indirect integration of the project's benefits.

Measure 4.2: Partners (especially SMEs) will seek to join forces with other businesses in order to promote the new hands-on training programme to existing customers or launch them in new sectors or geographical areas. This will be achieved through participation in international networking events (e.g., International Cyber Expo, Undersea Defense Technology event, Border Security Expo, Eurosatory etc.), as well as through marketing channels (email marketing, social media, business websites).

KPI	Target Value	Achieved during M1-M18
Partnership formed with key business in the field by the end of the project	≥10	N/A
Target group:	Project partners, partners' existing clientele	

Impact KPIs

Outcome / Impact | Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.

iKPI	Target Value	Achieved during M1-M18
iKPI-1: Number of EU Funded projects outcomes exploited by the end of the project	≥15	4
iKPI-5: Number of awareness workshops with end users	≥5	1
Target group:	Cyber security Providers, Cyber insurers and SMEs	

Outcome / Impact Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.		
iKPI	Target Value	Achieved during M1-M18
iKPI-6: Provide cyber insurance policies to SMEs for piloting purposes after the completion of the project at least for one year.	≥10 European SMEs	N/A
iKPI-7: Number of market-ready tools available in the Marketplace	≥15	N/A
iKPI-9: Number of engaging activities for opening the EU Cybersecurity Certification Ecosystem to SMEs	≥5	N/A
Target group:	SMEs, Organisations	

Outcome / Impact Improve the security of open-source solutions.		
iKPI	Target Value	Achieved during M1-M18
iKPI-10: Number of open-source communities engaged within ERMIS.	≥5	2 ¹¹
iKPI-12: Number of workshops/webinars organised for encouraging community participation.	≥5	1
iKPI-13: Number of security related contributions to open-source communities.	≥5	N/A
Target group:	Open-source cyber security solutions Providers	

¹¹ Open Source Observatory and Repository (OSOR) and Free and Open Source Software Auditing (FOSSA)

6. CONCLUSION

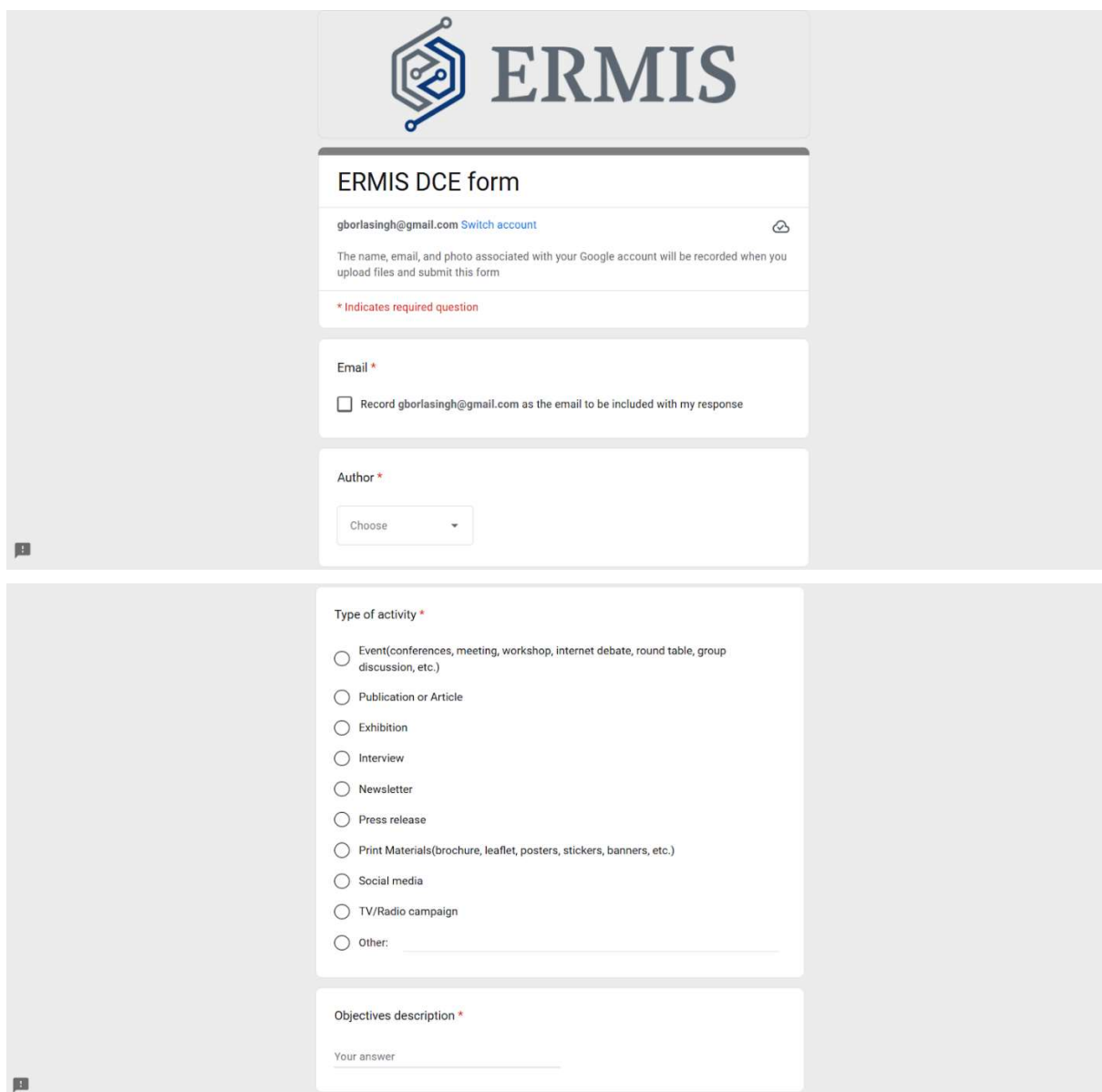
The ERMIS project has made substantial progress in implementing a dynamic and multi-pronged communication and dissemination strategy. Through coordinated efforts across the consortium, ERMIS has succeeded in raising awareness, engaging key stakeholders, and fostering dialogue within the cybersecurity and cyber insurance communities.

The strategic use of digital platforms, professional branding, and targeted events has ensured broad outreach and active participation from both primary and secondary stakeholder groups. The incorporation of feedback mechanisms and performance monitoring has allowed the consortium to refine its approach continuously, ensuring relevance and responsiveness to the evolving landscape.

Looking ahead, ERMIS will build upon this solid foundation by intensifying dissemination efforts, deepening stakeholder relationships, and advancing sustainability planning. The activities carried out and the insights gained during this reporting period provide a strong basis for achieving the project's long-term goals: promoting cybersecurity assurance, supporting the uptake of cyber insurance, and contributing to a more resilient European digital economy.

7. ANNEX 1

The following section displays the online form that is used to gather content for the social media and the website.



The screenshot shows the ERMIS DCE form interface. At the top, the ERMIS logo is displayed. Below it, the form title "ERMIS DCE form" is shown. The user's email "gborlasingh@gmail.com" is listed with a "Switch account" link. A note states: "The name, email, and photo associated with your Google account will be recorded when you upload files and submit this form". A red asterisk indicates required questions. The "Email" section has a checkbox for "Record gborlasingh@gmail.com as the email to be included with my response". The "Author" section has a dropdown menu labeled "Choose". The "Type of activity" section lists various options with radio buttons: Event(conferences, meeting, workshop, internet debate, round table, group discussion, etc.), Publication or Article, Exhibition, Interview, Newsletter, Press release, Print Materials(brochure, leaflet, posters, stickers, banners, etc.), Social media, TV/Radio campaign, and Other: (with a text input field). The "Objectives description" section has a text input field labeled "Your answer".

ERMIS DCE form

[gborlasingh@gmail.com](#) [Switch account](#)

The name, email, and photo associated with your Google account will be recorded when you upload files and submit this form

* Indicates required question

Email *

☐ Record gborlasingh@gmail.com as the email to be included with my response

Author *

Choose

Type of activity *

☐ Event(conferences, meeting, workshop, internet debate, round table, group discussion, etc.)

☐ Publication or Article

☐ Exhibition

☐ Interview

☐ Newsletter

☐ Press release

☐ Print Materials(brochure, leaflet, posters, stickers, banners, etc.)

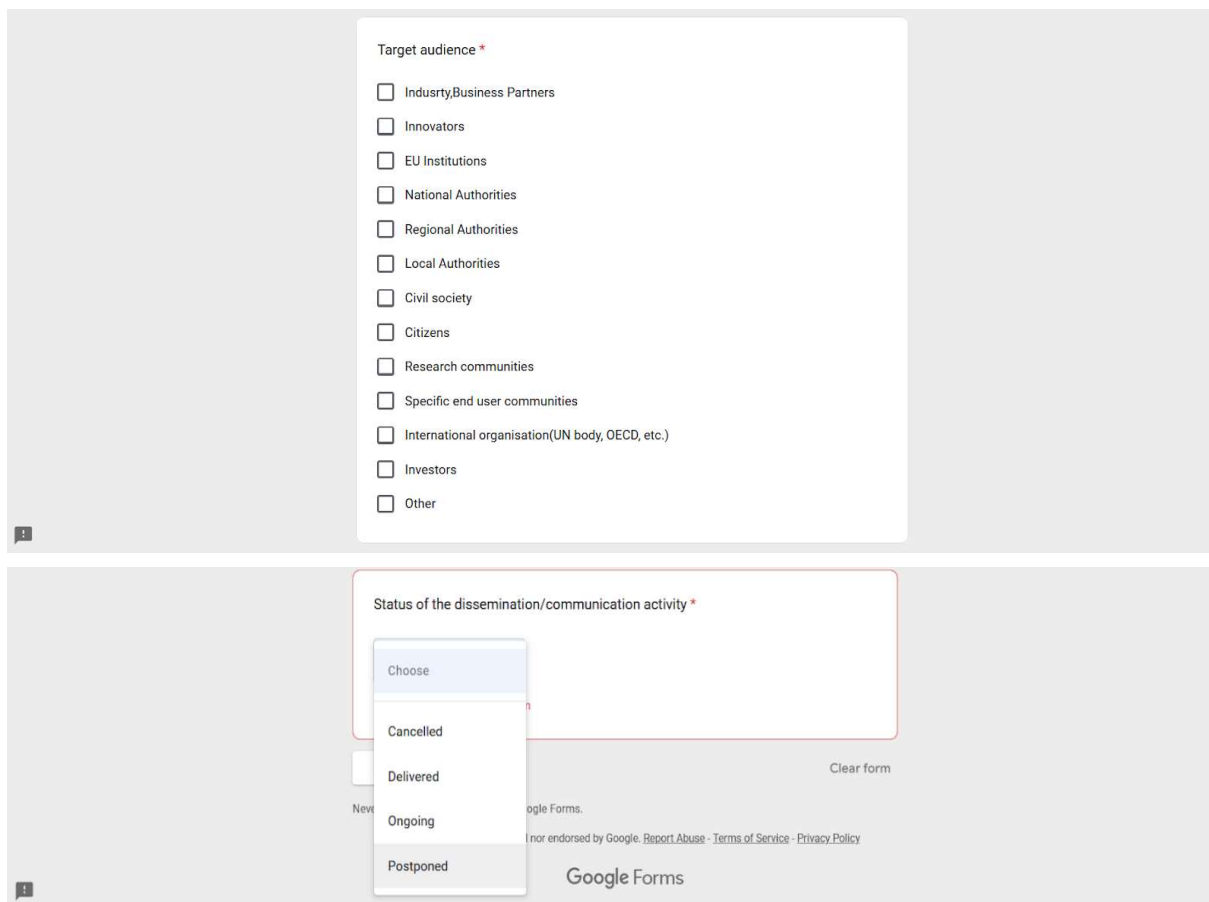
☐ Social media

☐ TV/Radio campaign

☐ Other: _____

Objectives description *

Your answer _____



The image shows two screenshots of a Google Form. The top screenshot displays a 'Target audience' section with a list of checkboxes for various groups: Industry, Business Partners; Innovators; EU Institutions; National Authorities; Regional Authorities; Local Authorities; Civil society; Citizens; Research communities; Specific end user communities; International organisation (UN body, OECD, etc.); Investors; and Other. The bottom screenshot shows the 'Status of the dissemination/communication activity' section with a dropdown menu open, listing options: Choose, Cancelled, Delivered, Ongoing, and Postponed. The form is hosted on Google Forms, and a 'Clear form' button is visible.

Target audience *

- ☐ Industry, Business Partners
- ☐ Innovators
- ☐ EU Institutions
- ☐ National Authorities
- ☐ Regional Authorities
- ☐ Local Authorities
- ☐ Civil society
- ☐ Citizens
- ☐ Research communities
- ☐ Specific end user communities
- ☐ International organisation (UN body, OECD, etc.)
- ☐ Investors
- ☐ Other


Status of the dissemination/communication activity *

Choose

- Cancelled
- Delivered
- Ongoing
- Postponed

Clear form

Google Forms

 **ERMIS**

ERMIS DCE form

gborlasingh@gmail.com [Switch account](#)

The name, email, and photo associated with your Google account will be recorded when you upload files and submit this form

Article / publication information


Website link
Provide us with the link to the full version the article or publication, if available

Your answer

[Back](#) [Next](#) [Clear form](#)

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

 **ERMIS**

ERMIS DCE form

gborlasingh@gmail.com [Switch account](#)

The name, email, and photo associated with your Google account will be recorded when you upload files and submit this form

Final details

Images
Remember: an image always grabs the readers' attention! If you have related images to accompany your text, add them here.
Note: Upload up to 10 images, not bigger than 100 MB, each.

[Add file](#)

Preferred posting date

Applies in the case of an event, if we need to post it in advance before the event occurs. In that case, don't forget to include the registration link in the "Related link" field, above.

Please note that we try to schedule the posts days (sometimes weeks) in advance, so we may not be able to satisfy the exact date requested here.

Make sure the date is in the future!

MM DD YYYY

__ / __ / ____

Other notes


Your answer

Back Next Clear form

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

 **ERMIS**

ERMIS DCE form

gborlasingh@gmail.com [Switch account](#)

The name, email, and photo associated with your Google account will be recorded when you upload files and submit this form

Untitled section

Thank you!
We will look into your request and post it soon!

A copy of your responses will be emailed to gborlasingh@gmail.com.

Back Submit Clear form

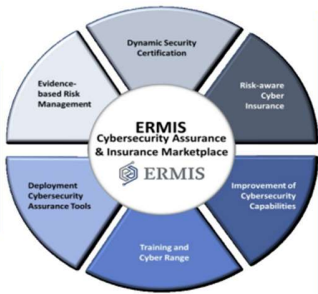
Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

8. ANNEX 2

The following section displays the presentation of ERMIS on December the 13th 2014.

ERMIS Vision




Target: Delivery of cyber security assurance and insurance as-a-service

Means: Integration of mechanisms, services, and tools into an innovative marketplace


Goals:

- Provide innovative cybersecurity insurance services
- Support the adoption of market-ready innovative cybersecurity solutions,
- Provide and deploy up to date tools and services to organisations
- Improve the security of open-source solutions.



Date: 13/12/2024 <https://dep-ermis.eu/> 4

ERMIS Objectives (1)




Obj. 1 – Design, implement and deliver a TRL-7 and highly usable cybersecurity, certification and cyber insurance management marketplace

Targeted end users: EU organisations, including SMEs, and public organisations, and cyber insurance agencies and relevant providers


Aim: Fostering the adoption and uptake of market-ready innovative cybersecurity solutions

- Provide a validated set of cybersecurity functional primitives as a service, to address security and privacy requirements of their composite cyber systems.
- Exploit and marketize the research outcomes and solutions developed in the framework of EU supported or funded projects
- Provide tailor-made services for cyber insurers, supporting the automated creation, pricing, continuous monitoring, and adaptation of cyber insurance policies for cyber systems.
- Increase the level of cybersecurity situation awareness and preparedness of SMEs
- Deliver an orchestrated ML-assisted environment



Date: 13/12/2024 <https://dep-ermis.eu/> 5

ERMIS Objectives (2)




Obj. 2 – Deliver market-ready tools for increasing the resilience and preparedness of SMEs against cyber threats

- Define and validate evidence-based risk, threat and vulnerability analysis ML-based models
- Enhance cyber-incident response among different digital infrastructures and cyber systems.
- Develop security audit and testing tools for discovering security flaws and improving the security of open-source solutions.

Obj. 3 – Deliver market-ready tools, processes and models for the agile and verifiable certification of cyber systems, ensuring the conformity assessment and validation

- Promote the scalable, agile and verifiable certification of cyber systems, towards ensuring and fostering the protection and resilience of SMEs products and services
- Optimize, automate and facilitate the conformity assessment of cyber systems ensuring compliance and mitigating potential compliance breaches.



Date: 13/12/2024 <https://dep-ermis.eu/> 6

ERMIS Objectives (3)



Obj. 4 – Deliver an innovative framework supporting the creation and management of cyber insurance policies and offering a sound liability basis for establishing trust in cyber systems and services

- Develop ML-based models for more accurate definition and specification of cyber insurance policies.
- Establish a process centric framework for automating the creation and management of cyber insurance policies for cyber systems.
- Establish conditions for improving cyber insurance practices and the trustworthiness of cyber systems and commercialising the use of the ERMIS platform and cyber insurance framework.

Obj. 5 – Validate the ERMIS offerings in real world environments and business cases for improving cybersecurity assurance capabilities in the EU and enhancing cyber insurance management

- Establish the evaluation process taking into account technical, usable, and techno-economic perspectives.
- Prove the applicability, usability, effectiveness and value of the ERMIS concepts, tools and services in the real-life business environment of European organisations and SMEs.

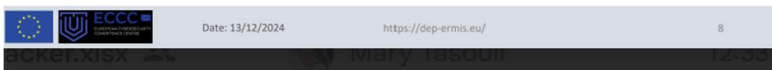


ERMIS Objectives

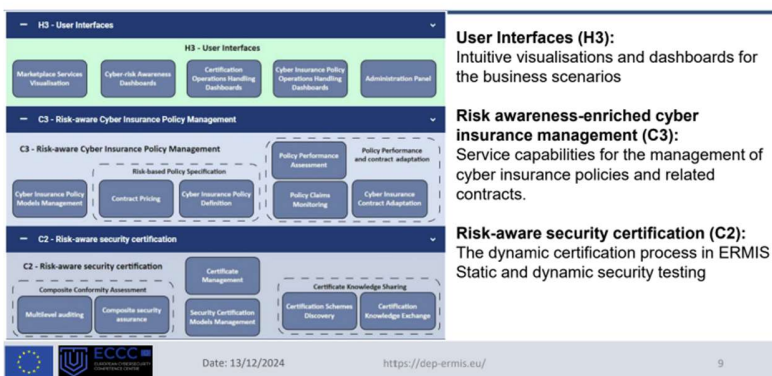


Obj. 6 –Raise awareness on the innovative ERMIS results to business, research, academic, and open-source communities in the EU and empower their skills in addressing ongoing cybersecurity challenges.

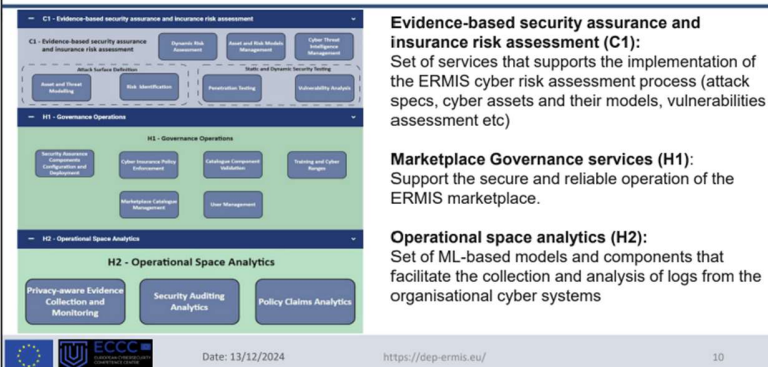
- Present the project progress, technologies and results to targeted stakeholders, ensuring wide awareness of main ERMIS marketplace users.
- Analyse the market for the ERMIS cybersecurity management framework, tools, services and solution, focusing on demand-driven exploitation scenarios.
- Deliver cyber ranges and training resources tailored to the needs of the cybersecurity and insurance experts.



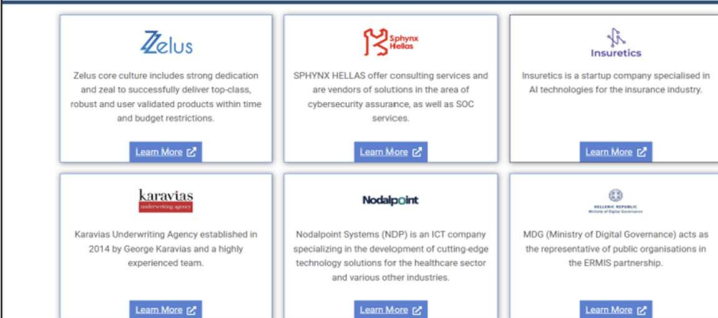
ERMIS Architecture (1)



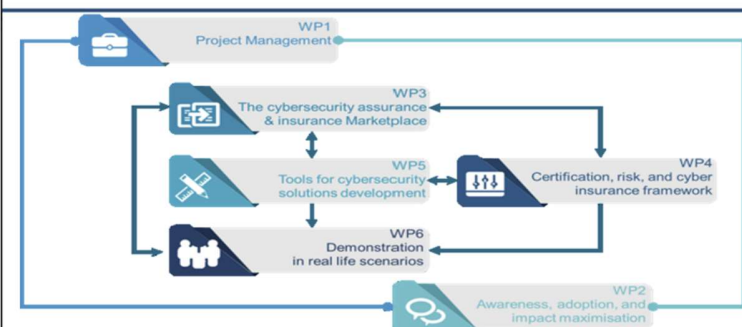
ERMIS Architecture (1)



ERMIS Consortium



ERMIS WorkPlan



ERMIS Expected Outcomes (1)



Target Group	Expected Benefits
Cyber Insurance Companies (primary)	Automated or semi- automated security certification and risk assessment. Reduce the information asymmetry between insurers and client
SMEs (primary)	Availability of tools, services and processes for cyber security assurance, certification and cyber insurance
Security services/tools Providers (primary)	Agile certification scheme ; Optimize security Challenges; certify tools/models/processes
Industry Associations	Regulation compliance; broad access to useful insights and tools
Scientific Community	Validated methods, tools, models and reference architecture



Date: 13/12/2024

<https://dep-ermis.eu/>

13

ERMIS Expected Outcomes (2)



Target Group	Expected Benefits
Open-source communities	Validation of security assurance of open-source components
Conformity Assessment Bodies	Certification models that incorporate risk management and cyber insurance of cyber systems
Policy Makers (primary)	Better insights on policy deficiencies and gaps; availability of conformity- related information
Consumer Associations & General Public	Secured and certified services, tools and processes



Date: 13/12/2024

<https://dep-ermis.eu/>

14

ERMIS Marketplace CS Insurance Services



ERMIS Static CS insurance policies

Static digital infrastructure image of organisations declared to Insurance Providers

ERMIS marketplace role:

- Broker of Insurance policies
- Risk Management assessment on quantifying cyber risks, understanding claims activity and staying ahead of evolving threats.
- User analytics and CS hardening recommendations.

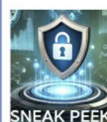
Challenged liability for the terms of the contract in case of a claim.

ERMIS CS Dynamic insurance policies

Dynamic monitoring of policy terms and digital infrastructure

ERMIS marketplace role:

- Broker of Insurance policies.
 - Risk Management advice on quantifying cyber risks, understanding claims activity, and staying ahead of evolving threats.
 - User analytics and general CS advice.
 - Provide CS assurance tools and services.
 - Continuous monitoring of policy terms.
 - Agents assurance in terms of a claim.
- Increased liability and overall risk reduction (premium and fine).



ERMIS Marketplace CS Assurance Services ERMIS

ERMIS Build-in Assurance tools

- Infrastructure monitoring services (logs and events) and detect
 - anomalies,
 - deviations,
 - and potential risks within the system
- Vulnerability and Penetration testing assessment services.


A Marketplace for other Assurance tools and services such as:

- Penetration testing tools
- Password auditing and packet sniffers
- Network defense
- Encryption
- Cyber Ranges



ERMIS Advanced certification processes

Real-time tracking of compliance with policies and controls targeting to:


- Streamlined compliance audits
- Increased trustworthiness and competitive edge / further reduced risk
- Transparency and accountability



SNEAK PEEK



Date: 13/12/2024 <https://dep-ermis.eu/> 16

 **ERMIS** Cybersecurity Assurance & Insurance Marketplace



Contact Us



Don't miss out on our news:

<https://dep-ermis.eu/>

or through email:

info@dep-ermis.eu



Date: 13/12/2024 <http://dep-ermis.eu/>  @DEP_ERMIS  DEP-Ermis

30/04/2025

51