Deliverable D6.5

Dissemination and Communication Report-v2

DRAFT

Editor(s):	Michela Fazzolari, Adriana Lazzaroni (CNR)
Responsible Partner:	Consiglio Nazionale delle Ricerche (CNR)
Status-Version:	Final v1.0
Date:	30.10.2026
Type:	R
Distribution level (SEN, PU):	PU

CC BY-SA

Project Number:	101120688
Project Title:	EMERALD

Title of Deliverable:	Dissemination and Communication Report-v2
Due Date of Delivery to the EC	31.10.2026

Workpackage responsible for the Deliverable:	WP6 – Dissemination, Exploitation and Communication
Editor(s):	Michela Fazzolari (CNR), Adriana Lazzaroni (CNR)
Contributor(s):	Patrizia Andronico Fabio Benedetti Raffaella Casarosa Michela Fazzolari, and Marinella Petrocchi (CNR) Juncal Alonso Cristina Martinez (TECNALIA) Björn Fanta (FABAR)
Reviewer(s):	Vanessa Komar (KNOW) Cristina Martinez, Juncal Alonso (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	All WPs

Abstract:	Second and last version of the report on the communication, dissemination and networking activities carried out during the second reporting period and the results obtained.
Keyword List:	Dissemination, communication, networking
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 4.0 International (**CC BY-SA 4.0 DEED** https://creativecommons.org/licenses/by-sa/4.0/)
Disclaimer	Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

DRAFT

(cc) BY-SA

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	16.03.2026	Table of Contents, first draft version	Michela Fazzolari (CNR)
v0.2	08.09.2026	Sections 2.1, 3.1, 3.1.1 and 3.1.2	Adriana Lazzaroni (CNR)
v0.3	20.09.2026	Second draft	Michela Fazzolari (CNR)
v0.4	21.09.2026	Section 3.3 and 3.4	Adriana Lazzaroni (CNR)
v0.5	13.10.2026	Sections 3.1.3 and 3.2	Adriana Lazzaroni (CNR), Fabio Benedetti (CNR), Raffaella Casarosa (CNR)
v0.6	19.10.2026	Added missing Figures, Appendices. Added material according to GA comments	Michela Fazzolari, Patrizia Andronico (CNR)
v0.7	21.10.2026	Complete revision done, deliverable ready for internal review	Michela Fazzolari (CNR)
v0.8	27.10.2026	QA review	Vanessa Komar (KNOW)
v0.9	28.10.2026	Address the comments from the QA review	Michela Fazzolari (CNR)
v1.0	30.10.2026	Final version submitted to the European Commission	Cristina Martínez, Juncal Alonso (TECNALIA)

DRAFT

CC BY-SA

Table of contents

Terms and Abbreviations 7
Executive Summary 8
1 Introduction 9
1.1 About this deliverable 9
1.2 Document structure 9
2 Global Progress and Results 11
2.1 Communication Results 11
2.2 Dissemination Results 12
2.3 Networking Results 13
3 Communication Activities 15
3.1 Digital Strategy 15
3.1.1 Project Website 15
3.1.2 EMERALD fragments 18
3.1.3 Websites analytics 22
3.2 Social Networks 24
3.2.1 X 25
3.2.2 LinkedIn 25
3.2.3 YouTube 26
3.3 Flyers 27
3.4 Press releases 28
4 Dissemination Activities 30
4.1 Publications 30
4.2 EMERALD News 33
4.3 Posters 33
4.4 Project showcases 34
4.5 Events 35
4.6 Presentations 39
4.7 Cloud Community Publications 41
5 Networking Activities 44
5.1 European Cluster for Cybersecurity Certification 44
5.1.1 Webinar “Innovation in Action: Strategies for Exploiting Horizon Europe Results” 47
5.1.2 Joint Exploitation Workshop 48
5.1.3 Global IoT Day Webinar and Roundtable 2026 49
5.1.4 Cross-Project Exploitation Workshop 50
5.1.5 2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools (LIFESEC 2026) 50

DRAFT

CC BY-SA

5.1.6 EC3 Project Webinar: From Research to Results 51
5.1.7 ETSI Security Conference 2026 – Panel "Certifying the Future: A Live Research Debate on Security Certification" 52
5.2 Networking with Other Initiatives 53
5.3 External Advisory Board 54
6 Final Assessment of KPIs 56
7 Conclusions 59
8 References 61
APPENDIX A Flyers 62
APPENDIX B Press Release in different languages 64
APPENDIX C EMERALD News 70
APPENDIX D Posters 76
APPENDIX E Presentation 77

List of tables

TABLE 1. EMERALD FRAGMENTS PUBLISHED IN THE SECOND PERIOD OF THE PROJECT 19
TABLE 2. LIST OF SCIENTIFIC PUBLICATIONS PRODUCED IN THE SECOND REPORTING PERIOD 31
TABLE 3. LIST OF EVENTS IN WHICH THE EMERALD PROJECT (OR PARTS OF IT) HAS BEEN ACTIVELY PRESENTED 36
TABLE 4. LIST OF THE EVENTS ATTENDED BY PARTNERS, WHOSE TOPICS ARE EMERALD-RELATED. 39
TABLE 5. EXPLANATION SYMBOLS FOR THE KPIS 56
TABLE 6. EMERALD KPIS FOR COMMUNICATION AND THEIR FINAL STATUS AT M36 56
TABLE 7. EMERALD KPIS FOR DISSEMINATION AND THEIR FINAL STATUS AT M36 57
TABLE 8. EMERALD KPIS FOR NETWORKING AND THEIR FINAL STATUS AT M36 57

List of figures

FIGURE 1. HOMEPAGE OF THE EMERALD WEBSITE 16
FIGURE 2. NETWORKING PAGE OF THE EMERALD WEBSITE 17
FIGURE 3. OPEN RESOURCES PAGE OF THE EMERALD WEBSITE 17
FIGURE 4. EMERALD FRAGMENTS PAGE 18
FIGURE 5. AN EXAMPLE OF AN EMERALD FRAGMENT 19
FIGURE 6. EMERALD WEBSITE ANALYTICS FROM MAY 2025 TO OCTOBER 2026 22
FIGURE 7. MOST VISITED PAGES OF THE EMERALD WEBSITE 22
FIGURE 8. VISITS TO THE EMERALD WEBSITE BY GEOGRAPHICAL LOCATION 23
FIGURE 9. COUNTRIES WITH THE HIGHEST NUMBER OF VISITS TO THE EMERALD WEBSITE 23
FIGURE 10. GLOBAL TRAFFIC ON THE EMERALD WEBSITE 24
FIGURE 11. TRAFFIC GENERATED BY SOCIAL NETWORKS 24
FIGURE 12. HOMEPAGE OF THE X ACCOUNT OF EMERALD 25
FIGURE 13. HOMEPAGE OF THE LINKEDIN PAGE OF EMERALD 26
FIGURE 14. ANALYTICS FOR THE LINKEDIN PAGE OF EMERALD OVER THE PAST 365 DAYS 26
FIGURE 15. HOMEPAGE OF THE YOUTUBE CHANNEL OF EMERALD 27
FIGURE 16. WEBPAGE DEDICATED TO PRESS RELEASES ON THE EMERALD WEBSITE 29
FIGURE 17. FIRST SLIDE OF THE PRESENTATION "EMERALD BLOCKCHAIN-BASED TRUSTWORTHINESS SYSTEM" 40

(cc) BY-SA

FIGURE 18. FIRST SLIDE OF THE PRESENTATION "CYBERSECURITY CERTIFICATION FOR THE COMPUTING CONTINUUM: FUTURE CHALLENGES AND OPPORTUNITIES" 40
FIGURE 19. FIRST SLIDE OF THE PRESENTATION "OSCAL IN THE EMERALD EU PROJECT" 41
FIGURE 20. PROJECTS CURRENTLY INVOLVED IN THE EC3 45
FIGURE 21. BLOG POSTS ON THE EC3 WEBSITE 46
FIGURE 22. EVENTS ON THE EC3 WEBSITE 47
FIGURE 23. PROMOTIONAL GRAPHIC FOR THE WEBINAR "INNOVATION IN ACTION: STRATEGIES FOR EXPLOITING HORIZON EUROPE RESULTS" 48
FIGURE 24. PARTICIPANTS AT THE JOINT EXPLOITATION WORKSHOP HELD IN ROME ON 20 NOVEMBER 2025 49
FIGURE 25. PROMOTIONAL BANNER FOR THE GLOBAL IOT DAY WEBINAR AND ROUNDTABLE 2026 50
FIGURE 26. SCREENSHOT OF PARTICIPANTS ATTENDING THE COCYBER CROSS-PROJECT EXPLOITATION WORKSHOP 50
FIGURE 27. PROMOTIONAL BANNER FOR THE 2ND WORKSHOP ON WHOLE-LIFECYCLE SECURITY FOR SMART SYSTEMS: METHODS AND TOOLS (LIFESEC 2026) 51
FIGURE 28. PROMOTIONAL BANNER FOR THE EC3 PROJECT WEBINAR "FROM RESEARCH TO RESULTS" 52
FIGURE 29. PROMOTIONAL BANNER FOR THE PANEL "CERTIFYING THE FUTURE: A LIVE RESEARCH DEBATE ON SECURITY CERTIFICATION" AT THE ETSI SECURITY CONFERENCE 2026 53
FIGURE 30. OUTER PANEL OF THE SECOND EMERALD FLYER 62
FIGURE 31. INNER PANEL OF THE SECOND EMERALD FLYER 62
FIGURE 32. OUTER PANEL OF THE THIRD EMERALD FLYER 63
FIGURE 33. INNER PANEL OF THE THIRD EMERALD FLYER 63
FIGURE 34. SECOND EMERALD PRESS RELEASE IN ENGLISH 64
FIGURE 35. SECOND EMERALD PRESS RELEASE TRANSLATED INTO FINNISH 65
FIGURE 36. SECOND EMERALD PRESS RELEASE TRANSLATED INTO GERMAN 66
FIGURE 37. SECOND EMERALD PRESS RELEASE TRANSLATED INTO ITALIAN 67
FIGURE 38. EMERALD PRESS RELEASE TRANSLATED INTO SPANISH 68
FIGURE 39. SECOND EMERALD PRESS RELEASE TRANSLATED INTO POLISH 69

DRAFT

(cc) BY-SA

Terms and Abbreviations

AI	Artificial Intelligence
CRA	Cyber Resilience Act
DoA	Description of Action
DORA	Digital Operational Resilience Act
EAB	External Advisory Board
EC3	European Cluster for Cybersecurity Certification
ECCO	European Cybersecurity COmmunity support project
EU	European Union
ETSI	European Telecommunications Standards Institute
IoT	Internet of Things
KPI	Key Performance Indicator
OSCAL	Open Security Controls Assessment Language
SEO	Search Engine Optimization
SME	Small and Medium Enterprise
URL	Uniform Resource Locator
WP	WordPress
WIP	Work In Progress
WP	Work Package

DRAFT

CC BY-SA

Executive Summary

This deliverable (D6.5) presents the final results of the communication, dissemination, and networking activities carried out within the EMERALD project, with particular emphasis on the second reporting period (M19–M36). Building on the strategy defined in D6.2 [1] and the activities documented in the Dissemination and Communication Report – v1 [2], it provides an overview of the actions undertaken, their outcomes, and the achievement of the corresponding Key Performance Indicators (KPIs).

Communication activities focused on increasing the project's visibility and ensuring that its objectives, progress, and results reached relevant target audiences. The EMERALD website remained the main communication channel, complemented by regular publications in the EMERALD fragments section and social media activities. During the second reporting period, approximately 40 fragments were published, while LinkedIn became the primary social media platform following the discontinuation of activities on X. Communication efforts were further supported by promotional materials, press releases, and videos, providing accessible information on the project and its technological developments.

Dissemination activities progressively shifted from presenting the project's objectives and initial developments towards sharing its scientific and technical results and demonstrating the practical applications of the EMERALD framework. The consortium contributed to scientific publications and participated in international conferences, workshops, webinars, and industrial events. Dedicated dissemination materials included two additional annual summaries, updated presentations, and eight additional videos, comprising an overview of the EMERALD framework, four UI/UX mock-ups, and three technical demonstrations of the main Compliance-as-a-Service functional streams. Particular attention was given to the dissemination of the results achieved during the final year, including the integration and validation of the framework and the audit activities carried out within the pilots.

Networking activities focused on strengthening collaboration with European research projects, industry representatives, standardisation bodies, and other relevant stakeholders. A major achievement was the consolidation and expansion of the European Cluster for Cybersecurity Certification (EC3), which evolved into an active platform for joint dissemination, technical cooperation, and exploitation activities. The cluster facilitated the organisation of webinars, workshops, and conference sessions, while technical collaboration progressed through the Collaborative Metrics Repository, supporting the reuse and interoperability of security metrics. In parallel, engagement with relevant European initiatives and the External Advisory Board (EAB) contributed to knowledge exchange and provided external perspectives on the project's technical developments and final results.

Overall, the communication, dissemination, and networking activities contributed to increasing the visibility of EMERALD, promoting the transfer of its research results, and strengthening collaboration within the European cybersecurity certification community. By combining complementary communication channels, scientific dissemination, technical demonstrations, and joint initiatives, the project supported the accessibility, uptake, and potential exploitation of its outcomes beyond its duration. The final assessment of the corresponding KPIs confirms that the project largely achieved its communication, dissemination, and networking objectives, with several indicators exceeding their initial targets.

DRAFT

CC BY-SA

1 Introduction

The objective of Work Package 6, "Dissemination, exploitation and communication", is to maximize the project's impact by ensuring effective communication, dissemination, and exploitation of its results, as well as contributing to relevant standardization efforts. These activities aim to raise awareness among scientific, industrial, and general public audiences and foster the adoption of the project's outcomes.

This deliverable presents the final results of the communication, dissemination, and networking activities carried out throughout the EMERALD project, with particular emphasis on the second reporting period (M19–M36). Building on the strategy defined in D6.2 [1] and the activities documented in the Dissemination and Communication Report – v1 [2], it provides an overview of the actions undertaken, their outcomes, and the final assessment of the corresponding Key Performance Indicators (KPIs). Please note that activities related to exploitation and standardisation are addressed separately in deliverable D6.7 [3].

1.1 About this deliverable

This deliverable provides a detailed account of the dissemination, communication, and networking activities carried out during the second reporting period of the EMERALD project (M19–M36). Its primary goal is to document the results achieved in raising awareness about the project, engaging with relevant stakeholders, and fostering collaboration within the scientific and industrial communities. It presents the outcomes of the activities undertaken and assesses their effectiveness against the defined KPIs.

The entire EMERALD consortium contributed to these activities, leveraging its diverse expertise and networks to maximise the project's visibility and impact. Partners participated in conferences, published research findings, organised events, and engaged with external stakeholders to support the dissemination of project results and promote their potential uptake beyond the project's duration.

1.2 Document structure

This document is structured as follows:

- Section 1 provides a general introduction, outlining the scope and structure of this deliverable.
- Section 2 presents a summary of the main results achieved in communication, dissemination, and networking activities throughout the second period of the project.
- Section 3 describes the communication activities carried out during the second reporting period. It covers the project's digital strategy, including the website, EMERALD fragments, and web analytics, as well as its presence on social media platforms such as X[1], LinkedIn[2], and YouTube[3]. It also reports on the communication materials produced, including flyers, press releases, and other communication activities.
- Section 4 covers dissemination activities, including scientific publications, annual summaries, posters, and project showcases. It also reports on participation in relevant events, the development and updating of presentation materials, and references to EMERALD from the broader scientific and industrial communities.
- Section 5 describes networking activities, focusing on the evolution of the European Cluster for Cybersecurity Certification (EC3), collaborations with other European

[1] https://x.com/EmeraldHEproj
[2] https://www.linkedin.com/company/emerald-he-project/
[3] https://www.youtube.com/@emerald-he-project

CC BY-SA

projects and relevant initiatives, and the activities and contributions of the External Advisory Board (EAB).

- Section 6 presents the final assessment of the communication, dissemination, and networking Key Performance Indicators (KPIs), comparing the results achieved throughout the project with the established targets.
- Section 7 presents the conclusions of the deliverable, summarising the main achievements and overall impact of the communication, dissemination, and networking activities.
- Finally, the Appendices provide supporting dissemination and communication materials, including flyers, press releases, annual summaries, posters, and presentation slides developed throughout the project.

DRAFT

(cc) BY-SA

2 Global Progress and Results

This section provides an overview of the main results achieved through communication, dissemination, and networking activities during the second reporting period of the EMERALD project (M19–M36).

2.1 Communication Results

The communication activities implemented within the EMERALD project have aimed at ensuring the visibility of the project and effectively communicating its activities, outputs, results, and expected impacts to relevant target audiences and stakeholders. To this end, the project has adopted a combination of communication channels and tools, considering both the characteristics of the target audiences and each channel's specific communication potential.

The project website has served as the main reference point for the project's communication and dissemination activities. It has provided stakeholders and interested audiences with access to information on the project, its objectives, activities, results, and expected impacts. In addition to general project information, dedicated sections make the main communication and dissemination outputs publicly accessible. In particular, the 'Communication' section provides access to the project flyers, press releases, annual summaries, presentations, videos, and posters developed throughout the project (see Section 3.1.1).

The website has been complemented by other digital communication channels, particularly the "EMERALD fragments" section and social media platforms. **Fragments have been a key feature of the project website**, providing detailed and accessible content on topics related to the partners' areas of expertise and the knowledge and capabilities developed through project activities. During the second reporting period, approximately 40 additional fragments were published on the website and shared through social media channels, contributing to the regular communication of project activities and results (see Section 3.1.2).

In addition, **promotional and demonstration videos were produced** to present the project's objectives, highlight its main benefits, and illustrate the functionalities and practical applications of the EMERALD framework. These videos, published on the project's YouTube channel (see Section 3.2) and described in greater detail under Project Showcases (see Section 4.4), have contributed to increasing awareness of the project and facilitating a better understanding of its solutions among different target audiences.

In the second reporting period, **social media have been employed to further increase the visibility and reach of EMERALD** and to facilitate interaction with relevant communities beyond the project consortium. These channels have enabled the project to engage with its target communities, other research projects, and members of the general public interested in cybersecurity, cloud computing, and security certification. Initially, LinkedIn and X were the main social media platforms used. However, the consortium discontinued its activity on X in June 2025, shifting its communication efforts primarily towards LinkedIn and YouTube. LinkedIn became the main social media channel for directing traffic to the EMERALD website, while YouTube was used primarily to share project videos and demonstrations (see Section 3.2).

Furthermore, **two additional flyers were produced during the second reporting period, representing an important communication tool** for presenting EMERALD's objectives, activities, and main achievements in an accessible and visually engaging format. These materials also highlighted the project's innovative approach to evidence management for continuous certification of cloud services and encouraged readers to visit the project website for further information (see Section 3.3).

CC BY-SA

Finally, during the second reporting period, **an additional press release was produced in six different languages**, presenting the project's main achievements and results, proving to be an essential communication tool for maintaining project visibility and engaging with a broad and diverse audience.

Overall, the combination of online channels and dedicated communication materials enabled EMERALD to reach different target audiences and communicate its progress and results through complementary formats. The use of these tools throughout the project contributed to strengthening its visibility and supporting engagement with relevant scientific, industrial, and wider communities.

2.2 Dissemination Results

The dissemination activities carried out within EMERALD aimed to share the project's research findings, technical developments, and results with relevant scientific and industrial communities, including researchers, industry professionals, policymakers, and stakeholders working in cybersecurity, cloud computing, and certification. Throughout the project, dissemination efforts progressively shifted from presenting the project's objectives and initial developments towards sharing more mature technical results, demonstrating the functionalities of the EMERALD framework, and highlighting its application and validation in real-world environments.

Scientific publications represented a key component of the dissemination strategy. During the first 18 months, five publications were produced, including one journal paper and four conference contributions, as documented in the previous version of the Dissemination and Communication Report [2]. During the second reporting period, **nine additional scientific publications contributed to advancing research** in areas such as automated compliance assessment, security metrics, evidence management, and cloud cybersecurity certification. Further papers were also submitted for publication, extending the dissemination of the project's research results beyond its duration. A detailed overview of all publications produced during the second reporting period is provided in Section 4.1.

The consortium also actively **participated in national and international conferences, workshops, seminars, webinars, and industrial events**, presenting research findings and demonstrating the project's technological developments. These activities provided opportunities to engage with scientific and industrial stakeholders, exchange knowledge, and gather feedback on the approaches developed within EMERALD. During the final reporting period, particular attention was given **to presenting the project's results and their potential applications**, including contributions to international conferences and events addressing cybersecurity certification, cloud security, and compliance automation (see Section 4.5).

A range of **dedicated materials was developed to support the dissemination of project results** to different audiences. During the second reporting period, **two additional annual summaries were produced**, providing accessible overviews of the progress and achievements of the second and third years of the project. The final edition placed particular emphasis on the pilot activities, including the application and validation of the EMERALD framework and the audit processes carried out during the final year (see Section 4.2).

Following the three posters produced during the first reporting period [2], an additional scientific poster was developed for KEOD 2026 to support the dissemination of EMERALD's research results (see Section 4.3). In parallel, **presentation materials were updated and expanded** to reflect the project's technical progress and final results (see Section 4.6).

(cc) BY-SA

Project showcases represented another important dissemination tool, particularly during the second reporting period. Building on the two introductory videos produced during the first 18 months, **eight additional videos were developed** to illustrate the EMERALD framework and its practical applications. These included an overview of the framework, four UI/UX mock-up videos illustrating the envisioned user interactions, and three technical demonstration videos showing the actual implementation of the main functional streams of the Compliance-as-a-Service solution: Certification Schemes, Targets of Evaluation, and Audit Scopes. These materials facilitated a better understanding of the developed solutions and their practical use by different stakeholders (see Section 4.4).

Finally, the dissemination of EMERALD's results was further **supported by references to the project on external websites, research platforms, and other European initiatives**. These mentions contributed to increasing the project's visibility within the broader cybersecurity and cloud certification communities and reflected its involvement in collaborative research and dissemination activities (see Section 4.7).

Overall, the dissemination activities carried out throughout EMERALD contributed to sharing the project's scientific and technical results, increasing their visibility among relevant stakeholders, and promoting knowledge transfer beyond the consortium. The combination of scientific publications, conference participation, annual summaries, presentations, and demonstration videos enabled the project to communicate its results through complementary formats, supporting their accessibility and potential reuse by the wider research and industrial communities.

2.3 Networking Results

Networking activities within EMERALD focused on strengthening collaboration with European research projects, industry representatives, standardisation bodies, and other relevant stakeholders in the fields of cybersecurity, cloud computing, and certification. Building on the relationships established during the first 18 months, the second reporting period placed particular emphasis on joint technical activities, knowledge exchange, and the exploitation of research results, with the aim of promoting synergies and supporting the potential uptake of the solutions developed within the project.

A major achievement was the consolidation and expansion of the **European Cluster for Cybersecurity Certification (EC3)**, established during the first reporting period. The cluster expanded its membership to nine European research projects, bringing together complementary expertise in continuous certification, automated compliance, cloud and IoT security, and conformity assessment. During the second reporting period, EC3 evolved into an active collaboration forum, facilitating joint dissemination and exploitation activities through webinars, workshops, and conference sessions. Notable initiatives included the Global IoT Day 2026 webinar, the LIFESEC 2026 workshop, the final EC3 Project Webinar, and a joint panel at the ETSI Security Conference 2026. In addition, several exploitation-oriented workshops provided opportunities to exchange experiences, identify complementarities among project results, and explore potential pathways for their uptake and long-term sustainability (see Section 5.1).

Technical collaboration also progressed through the development of the **Collaborative Metrics Repository (CMR)**, a shared resource supporting the definition, maintenance, and reuse of security metrics across participating projects. EMERALD contributed to this initiative and integrated the repository into its framework, promoting consistency and interoperability in cybersecurity compliance assessment. The cluster also supported the **EUROSCAL initiative**,

(cc) BY-SA

fostering the adoption of machine-readable security requirements and automated compliance approaches based on the Open Security Controls Assessment Language (OSCAL).

Beyond EC3, EMERALD maintained engagement with relevant European initiatives and standardisation activities, particularly through its collaboration with the **European Telecommunications Standards Institute (ETSI)**[4]. These interactions contributed to exchanging research findings and aligning the project's technical developments with broader European efforts in cybersecurity certification and standardisation.

Finally, the **External Advisory Board (EAB),** established during the first reporting period, continued to provide an important channel for engagement with external experts from academia, industry, and standardisation. Four additional meetings were organised between M19 and M36, focusing on specific technical developments, including *CertGraph*, the EMERALD User Interface and User Experience, EC3, and the Collaborative Repository of Metrics. The final meeting focused on the EMERALD framework as an integrated solution, paying particular attention to its main components, exploitation potential, and long-term sustainability. These sessions provided opportunities to exchange knowledge, gather external perspectives, and discuss the potential applications of the developed solutions (see Section 5.3).

Overall, the networking activities carried out during the second reporting period strengthened EMERALD's connections with the wider European cybersecurity research and innovation community. Through joint initiatives, technical collaboration, and engagement with external experts, the project contributed to promoting knowledge exchange, interoperability, and opportunities for continued cooperation beyond its duration.

DRAFT

[4] https://www.etsi.org/

CC BY-SA

3 Communication Activities

This section reports the results of the communication activities carried out during the second reporting period (M19–M36) of the EMERALD project. Building on the strategy defined in deliverable D6.2 [1] and the activities documented in the previous version of the Dissemination and Communication Report [2], communication efforts focused on promoting the project's progress, technical developments, and results among relevant target audiences.

These activities encompassed a range of communication channels and materials, including the management and regular updating of the project website, the publication of EMERALD fragments, social media activities, and the production of flyers, videos, and press releases. Together, these tools supported the continuous communication of project developments and achievements, highlighting the added value and potential benefits of EMERALD for its target audiences.

The communication activities addressed the key stakeholder groups identified in D6.2 [1], including Cloud Service Providers (CSPs), auditors, National Cybersecurity Certification Authorities (NCCAs), the research and technical community, ENISA, as well as the general public and cloud service users.

The effectiveness of these activities was monitored throughout the project through the relevant KPIs. The final assessment of the communication KPIs and their achievement against the established targets is provided in Section 6.

3.1 Digital Strategy

The EMERALD Digital Strategy was successfully implemented throughout the project, relying primarily on the project website, the regular publication of EMERALD fragments, and the use of social media platforms, particularly LinkedIn and YouTube. Initially, X was also part of the communication strategy, but its use was discontinued in June 2025 to concentrate communication efforts on channels more closely aligned with the project's target audiences.

The EMERALD fragments (see Section 3.1.2) and social media channels played a complementary role within the communication strategy, serving both as a means of sharing project-related knowledge and as a tool for attracting and engaging visitors to the website. New fragments and other relevant content published on the website were regularly promoted through LinkedIn, with direct links to the corresponding pages.

Throughout the project, the coordinated use of these digital channels enabled the regular communication of project developments and achievements, including updates on the EMERALD framework, demonstration videos, public deliverables, press releases, General Assemblies, and other relevant activities. This approach contributed to increasing the accessibility and visibility of project results, facilitating engagement with the target communities and supporting a broader understanding of EMERALD's objectives and technological solutions.

3.1.1 Project Website

The EMERALD website, established at the beginning of the project, **has served as the main platform for communicating project activities, developments, and results to external audiences** (https://www.emerald-he.eu/).

The website and its different sections (see Figure 1) provide information on the project's organisation, objectives, vision, proposed solutions, key features, use cases, and main results. In addition, the platform hosts the “EMERALD fragments”, described in Section 3.1.2.

CC BY-SA

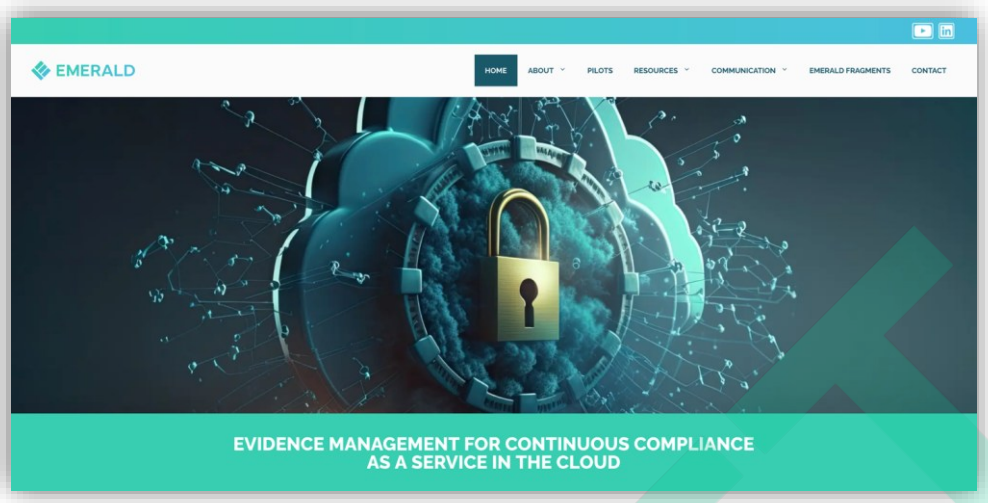


Figure 1. Homepage of the EMERALD website

The website structure, described in the Dissemination and Communication Report – v1 [2], remained substantially unchanged during the second reporting period. Nevertheless, several sections were regularly updated with new materials, including scientific publications, public deliverables, annual summaries, flyers, presentations, videos, and information on networking activities. In addition, new sections were introduced to accommodate further project outputs and developments.

In July 2025, **a new subsection entitled "Standardization"[5] was introduced** under the "Resources" section. This subsection presents EMERALD's contributions to standardization activities and its efforts to promote interoperability and the adoption of common approaches to cybersecurity compliance. It focuses on three main areas:

- OSCAL integration
- the Common Metrics Repository
- engagement with the European Telecommunications Standards Institute (ETSI).

The subsection previously named "Synergies", also located under "Resources", **was renamed "Networking"[6].** This section highlights EMERALD's contribution to the establishment and development of the **European Cluster for Cybersecurity Certification (EC3)**, an initiative aimed at fostering collaboration among European research projects, exchanging experiences, aligning methodologies, and promoting a common perspective on cybersecurity certification (see Figure 2). The page also contains a table which includes a set of projects with which EMERALD collaborates and details the networking activities that have taken place to date.

[5] https://www.emerald-he.eu/standardization/
[6] https://www.emerald-he.eu/networking/

(cc) BY-SA

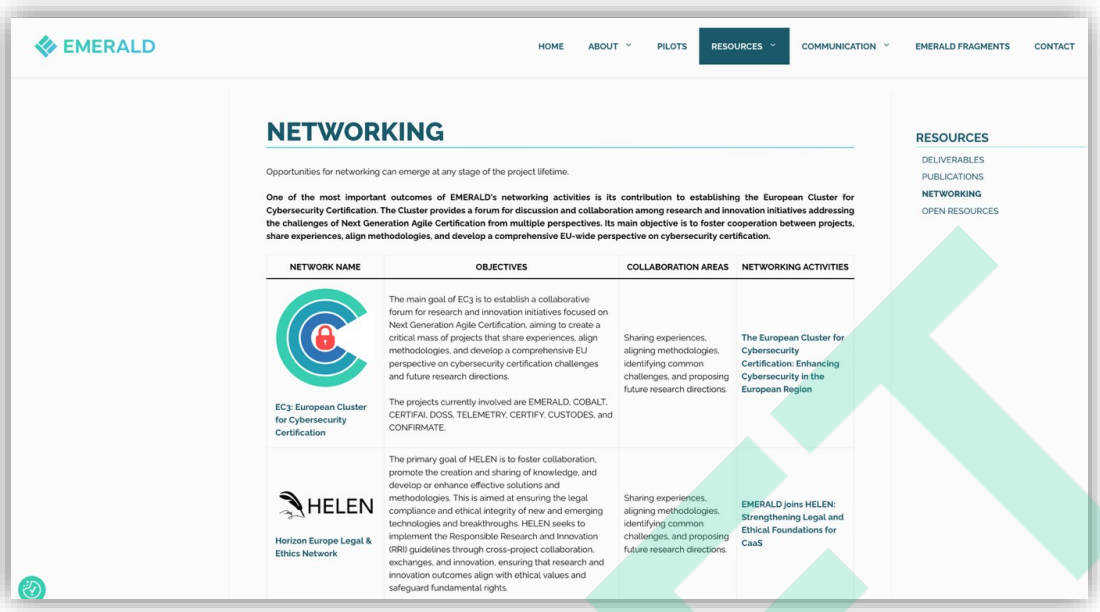


Figure 2. Networking page of the EMERALD website

The **"Open Resources"** subsection (see Figure 3) was also expanded to provide access to additional external resources. In particular, it includes a link to **GitLab**[7], where the public source code repositories developed within EMERALD are hosted, and to the EMERALD community on **Zenodo**[8], an open-access repository providing access to public deliverables, annual summaries, flyers, and other project materials.

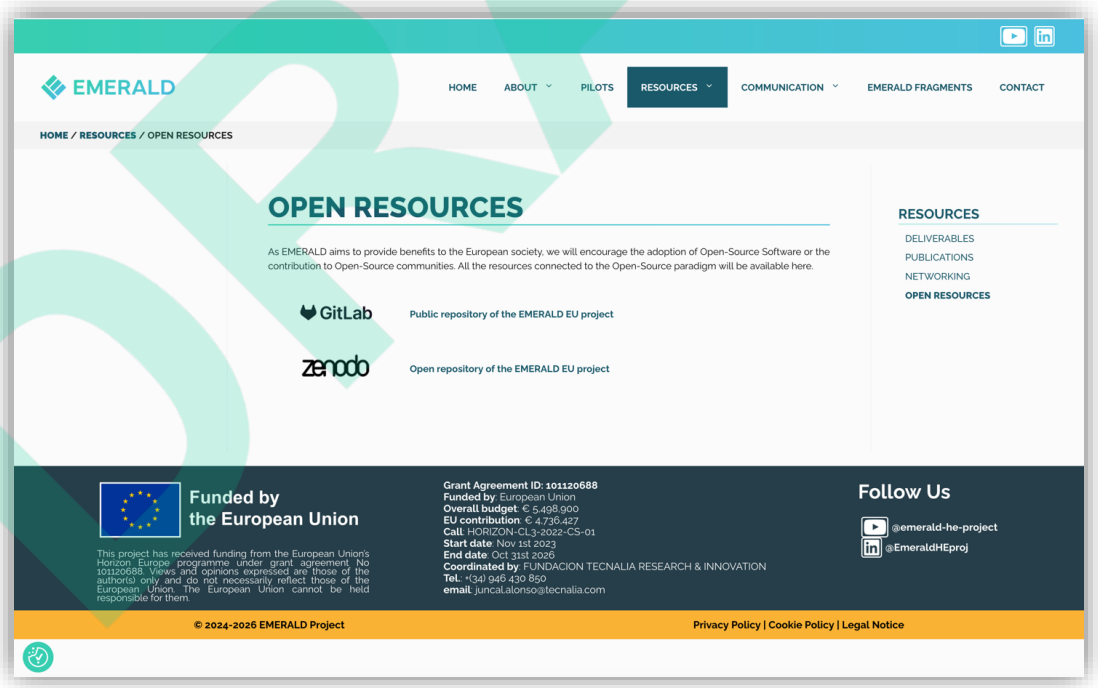


Figure 3. Open resources page of the EMERALD website

[7] https://git.code.tecnalia.dev/emerald/public
[8] https://zenodo.org/communities/emerald-he-project

CC BY-SA

Furthermore, following discussions held during the General Assembly in Pisa, the consortium agreed to **adopt the term "compliance" instead of "certification"** in the project's communication materials, including the reinterpretation of the **CaaS acronym as "Compliance-as-a-Service**". This terminology better reflects the scope of the EMERALD framework and its focus on supporting continuous compliance assessment processes. While the terminology in official project documents remained unchanged, the updated wording was progressively introduced across project's deliverables and communication channels, particularly on the website homepage, the sections dedicated to key results and pilots, and social media publications.

3.1.2 EMERALD fragments

The "EMERALD fragments" represented one of the main communication channels adopted by the project to provide regular and targeted information to its audience. Fragments are concise pieces of project-related information, written in an accessible style and complemented by images, links to additional content, and references to relevant pages of the project website (see Figure 4). To facilitate the identification and retrieval of information, the published fragments were organised into seven different categories according to the type of content addressed.

As described in the Dissemination and Communication Report – v1 [2], **fragments were published on a monthly basis,** with a target of at least two contributions per month, in a dedicated section of the project website[9]. All project partners contributed to this activity according to the "Social Media/Fragments Rotation Schedule", which helped maintain a regular flow of content and ensured contributions from across the consortium.

The selection of topics was left to the contributing partners, who identified the aspects of the project most relevant to their respective activities and responsibilities. Fragments provide insights into specific areas of project implementation and results, including use cases, architectures, frameworks, tools, deliverables, networking activities, events, and cloud services.

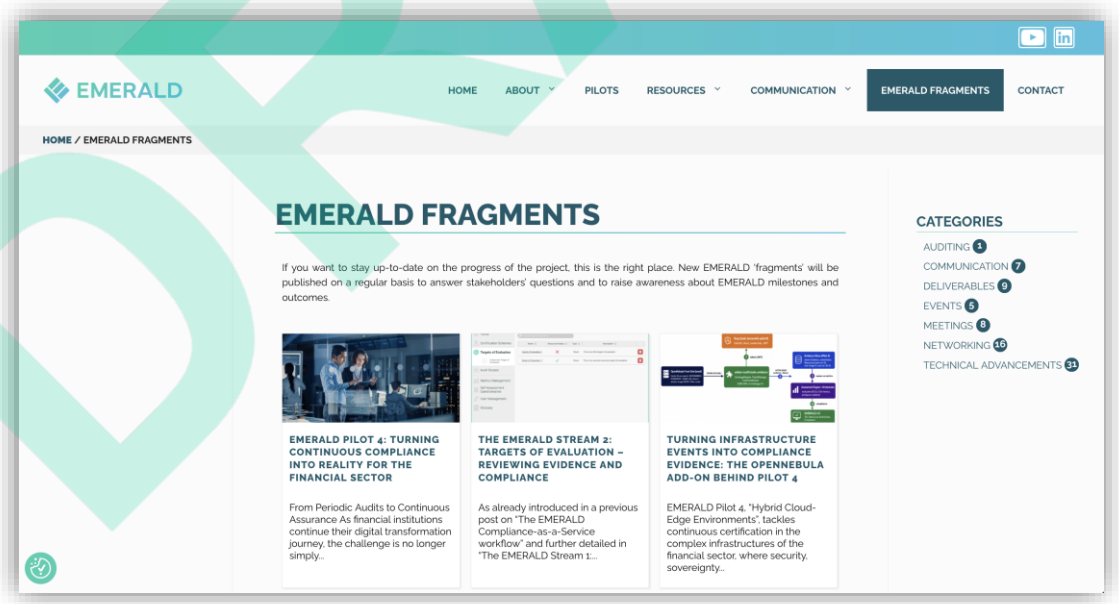


Figure 4. EMERALD fragments page

[9] https://www.emerald-he.eu/emerald-fragments/

(cc) BY-SA

In addition to their publication on the project website, the EMERALD fragments were actively promoted through the project's social media channels to further increase their visibility and reach. Initially shared through both X and LinkedIn, fragments were subsequently promoted primarily through LinkedIn following the discontinuation of activity on X in June 2025 (see Section 3.2). Figure 5 shows an example of an EMERALD fragment page, which addresses the topic "Standardizing Cloud Compliance".

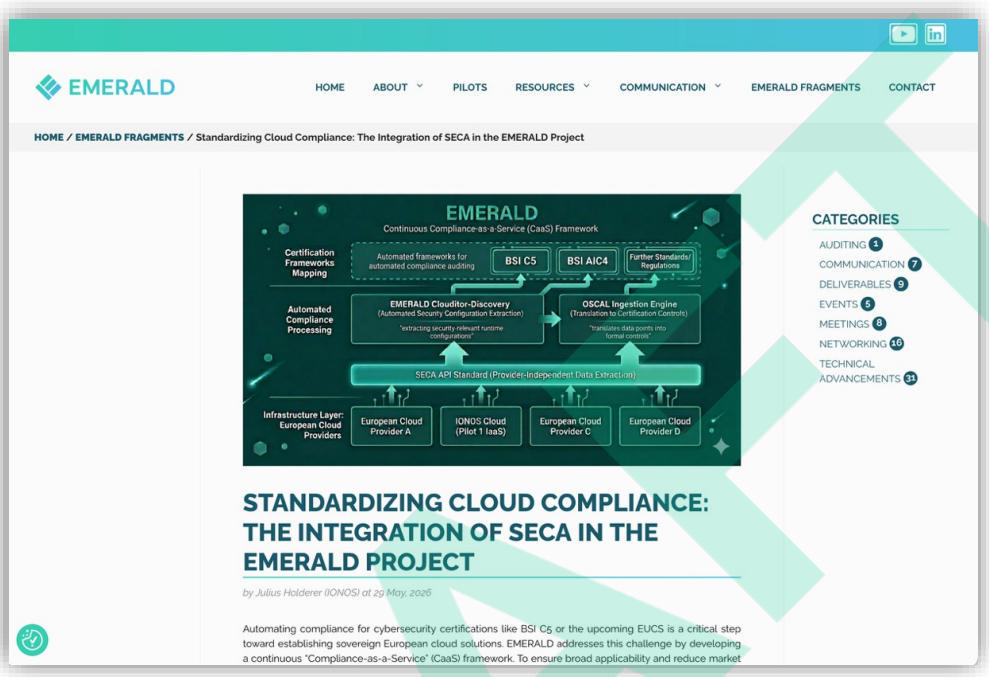


Figure 5. An example of an EMERALD fragment

During the second reporting period (M19–M36), **approximately 40 fragments were published** in the dedicated "EMERALD fragments" section of the project website. **This result exceeded the target established by the corresponding KPI,** demonstrating the effectiveness of this communication channel in sharing project-related information, activities, and results.

Table 1 provides an overview of the fragments published during the second reporting period, including their titles, main authors, publication dates, and direct links to the corresponding content on the project website.

Table 1. EMERALD fragments published in the second period of the project

#	Fragment Title	Author	Release date
1	EMERALD and other E3C Projects Successfully Hosted a Panel on Cybersecurity Certification at CLOSER 2025	Juncal Alonso, Cristina Martinez (TECNALIA)	7 May, 2025
2	From thorough preparation to the icing on the cake – audit preparation processes at IONOS	Julius Holderer (IONOS)	8 May, 2025
3	EMERALD contributes to the global IoT Day 2025	Michela Fazzolari (CNR)	14 May, 2025
4	Seven new deliverables published on 30th April 2025!	Adriana Lazzaroni (CNR)	14 May, 2025

(cc) BY-SA

#	Fragment Title	Author	Release date
5	Multi-Cloud with OpenNebula: Working on a DORA-Ready Blueprint for Resilient Banking	Jordi Guijarro (ONS)	3 June, 2025
6	New Developments in the CertGraph Ontology	Stefan Schöberl (SCCH)	26 July, 2025
7	MARI: Mapping Assistant for Regulations with Intelligence	Marinella Petrocchi (CNR)	9 September, 2025
8	Secure and Sovereign Cloud	Björn Fanta (FABAR)	29 September, 2025
9	EMERALD joins HELEN: Strengthening Legal and Ethical Foundations for CaaS	Michela Fazzolari (CNR)	30 September, 2025
10	The 2nd EMERALD Flyer is released	Adriana Lazzaroni (CNR)	1 October, 2025
11	From Auditors Desk: Why Architecture Diagrams and Documentation Are Essential in the Audit Process	Antti Kantero (DNV Cyber)	9 October 2025
12	EMERALD metrics migration progress	Angelika Schneider (FHG)	11 October, 2025
13	The EMERALD Co-Creation & Co-Design Process	Angela Fessl (KNOW)	16 October, 2025
14	The Emerald consortium met in Linz for the 6th General Assembly	Michela Fazzolari (CNR)	17 October, 2025
15	AI-SEC Tool Development Progress	Ching-Yu Franziska Kao (FHG)	29 October, 2025
16	EMERALD solution architecture	Iñaki Etxaniz (TECNALIA)	18 November, 2025
17	The EMERALD Compliance-as-a-service Workflow	Angela Fessl (KNOW)	25 November, 2025
18	eknows-e3 Development Progress	Stefan Schöberl (SCCH)	25 November, 2025
19	Software Provenance for Cloud Services	Angelika Schneider (FHG)	1 December, 2025
20	EU Projects Joint Workshop on Exploitation & Technical Collaboration	Franz Deimling, Björn Fanta (FABAR)	3 December, 2025
21	EMERALD and CUSTODES Join Forces to Explore Synergies and Collaboration	Michela Fazzolari (CNR), Cristina Martinez (TECNALIA)	19 December, 2025
22	The Second EMERALD Annual Summary Is Now Available	Michela Fazzolari (CNR)	15 January, 2026
23	Strengthening Financial Resilience: Why EMERALD is Leading the Way	Martí Fabregat, Ramon Martín De Pozuelo (CXB), Pablo del Arco, Jordi Guijarro, Bruno Rodriguez (ONS)	28 January, 2026

(cc) BY-SA

#	Fragment Title	Author	Release date
24	The EMERALD Stream 1: Certification Schemes – Structuring Compliance Through Metrics Mapping	Katharina Stefan, Angela Fessl (KNOW)	31 January, 2026
25	3rd Cohort of the European Blockchain Sandbox Best Practices for the EMERALD Trustworthiness System	Cristina Regueiro (TECNALIA)	25 February, 2026
26	Are We Ready for Audits?	Jari Temonen (DNV Cyber)	13 March, 2026
27	The EMERALD Consortium Met in Munich for the 7th General Assembly	Michela Fazzolari (CNR)	16 March, 2026
28	Integrating Semantic Technologies into Microservices with owl2proto	Angelika Schneider (FHG)	9 April, 2026
29	Validation Preparation	Franz Deimling (FABAR)	10 April, 2026
30	From Security Metrics to Ontology Evolution with AIOX	Verena Geist (SCCH)	28 May, 2026
31	Standardizing Cloud Compliance: The Integration of SECA in the EMERALD Project	Julius Holderer (IONOS)	29 May, 2026
32	The EMERALD Consortium met in Warsaw for the 8th General Assembly	Natalia Sobieska (CF)	16 June, 2026
33	Turning Infrastructure Events into Compliance Evidence: the OpenNebula Add-on Behind Pilot 4	Pablo del Arco, Jordi Guijarro, Bruno Rodriguez (ONS)	13 July, 2026
34	The EMERALD Stream 2: Targets of Evaluation – Reviewing Evidence and Compliance	Vanessa Komar, Katharina Stefan, Angela Fessl (KNOW)	27 July, 2026
35	Emerald pilot 4: turning continuous compliance into reality for the financial sector	Martí Fabregat, Ramón Martín de Pozuelo (CXB), Pablo del Arco, Jordi Guijarro, Bruno Rodríguez (ONS)	31 July, 2026
36	Putting EMERALD to the Test: Lessons from EMERALD's First Real-World Audit with IONOS Pilot	Netsanet Haile Gebreyesus, Julius Holderer (IONOS)	30 September, 2026
37	The 3rd EMERALD Flyer is released	Michela Fazzolari (CNR)	15 October, 2026
38	EMERALD Consortium Meets in Bilbao for Its Final General Assembly	Michela Fazzolari (CNR)	19 October, 2026
39	Pilot 2 – Finding Organisational Evidence with AMOE	Natalia Sobieska (CF)	20 October, 2026
40	The 3rd EMERALD Annual Summary is Now available	Michela Fazzolari (CNR)	22 October, 2026
41	EMERALD Pilot Audits Show the Value of Evidence-Based Cloud Compliance	Jari Temonen, Markus Pitkaranta, Mika Leskinenn (DNV Cyber)	27 October, 2026

(cc) BY-SA

3.1.3 Websites analytics

The EMERALD website uses the third-party plugin WP Statistics[10] to monitor website activities. According to the analytics data collected as of the end of October 2026 (see Figure 6), in the second reporting period the number of visits to the EMERALD website was about 4,000. **Throughout the whole period of operation of the website, EMERALD has maintained a stable number of daily users**, with increases observed whenever relevant activities occur, such as the publication of a "fragment" post.

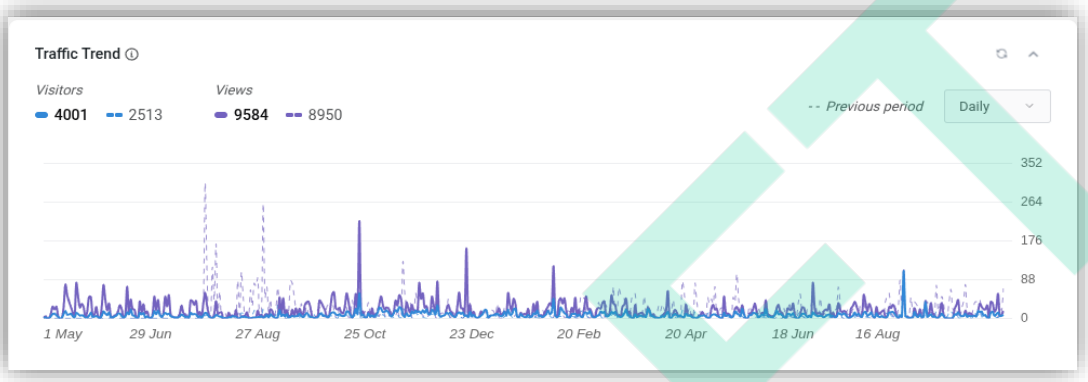


Figure 6. EMERALD website analytics from May 2025 to October 2026

In the second reporting period, articles published in the "EMERALD fragment" section continued to attract visitors to the project website. Indeed, as shown in Figure 7, the "EMERALD fragment" section was the second most visited page after the homepage, recording 885 page views, corresponding to 9.2% of the total 9,584 website visits.

Page	Visitors	Views	Words
HOME	2,148	3,269	268
EMERALD FRAGMENTS	540	885	216
DELIVERABLES	370	487	0
PARTNERS	240	288	1,479
PUBLICATIONS	172	206	355
PILOTS	163	209	290
MISSION	151	177	132
FLYERS	99	122	0
OPEN RESOURCES	95	122	48
NETWORKING	92	132	1

Figure 7. Most visited pages of the EMERALD website

[10] https://it.wordpress.org/plugins/wp-statistics/

CC BY-SA

Regarding the **geographical distribution of EMERALD's audience**, the countries with the highest number of visitors are China, Italy, USA and Austria, as shown in Figure 8 and Figure 9. The publication of the EMERALD press release in six different languages has probably contributed to increase the traffic from different countries.

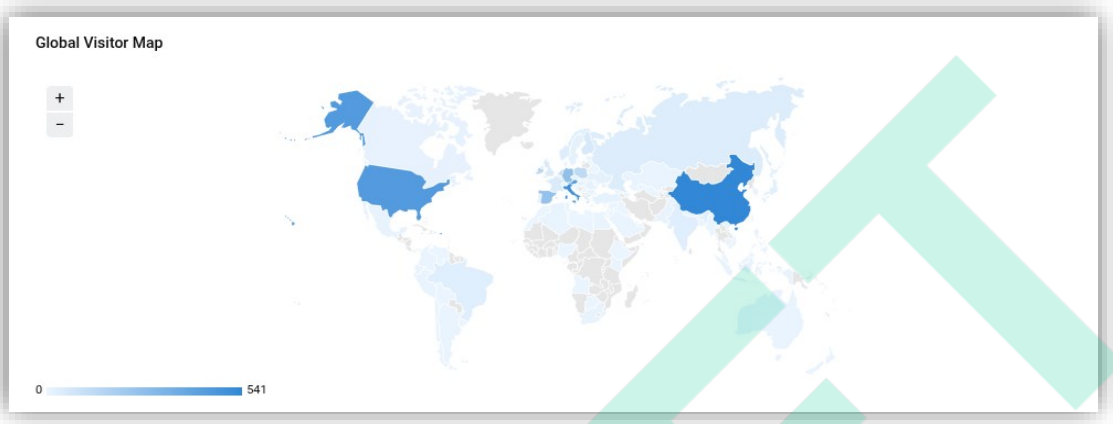


Figure 8. Visits to the EMERALD website by geographical location

Country	Visitors	Views
China	541	549
Italy	495	2,467
United States	445	752
Austria	437	1,472
Singapore	347	358
Germany	264	800
Spain	247	829
Ireland	153	236
Netherlands	145	224
Poland	133	405

Figure 9. Countries with the highest number of visits to the EMERALD website

Search Engine Optimization (SEO) performance kept improving thanks to the provision of dedicated and targeted content through the fragments and social media. As shown in Figure 10, visits from direct search queries represent about 76.4% of the traffic, while 19.1% of visitors come from organic searches, 0.5% from social networks and 0.1% from email. Direct searches allow users to access the site directly by typing the URL into the browser bar. Organic searches are made by users who search for the site and reach it through search engines.

(cc) BY-SA



Figure 10. Global traffic on the EMERALD website

In terms of visitors coming from social networks (see Figure 11), **LinkedIn has been the main channel used to access the EMERALD website.**



Figure 11. Traffic generated by social networks

3.2 Social Networks

The EMERALD social media channels were primarily used to direct traffic to the project website, where more detailed information and project-related content were made available. Regular updates concerning technical developments, project outcomes, news, and events were shared through these channels. The following subsections provide an overview of how each social media platform was used to support the communication and promotion of EMERALD activities.

(cc) BY-SA

3.2.1 X

During the first reporting period, X was one of the main social media platforms used by EMERALD, alongside LinkedIn and YouTube. The project's X account, **@EmeraldHEproj**, was created in November 2023, shortly after the start of the project (see Figure 12). Posts included original content, such as participation in events, EMERALD fragments, press releases, as well as reposts of relevant content from external stakeholders.

By 28 April 2025, the account had reached 34 followers and 55 posts, remaining below the initial KPI target of 200 followers. This limited performance was attributed in part to changes in the platform's user base and its decreasing relevance for reaching professionals interested in research and innovation.

Consequently, in June 2025, the consortium decided to discontinue communication activities on X and concentrate its efforts on LinkedIn and YouTube, which were considered more suitable for reaching the project's target audiences and sharing its results.

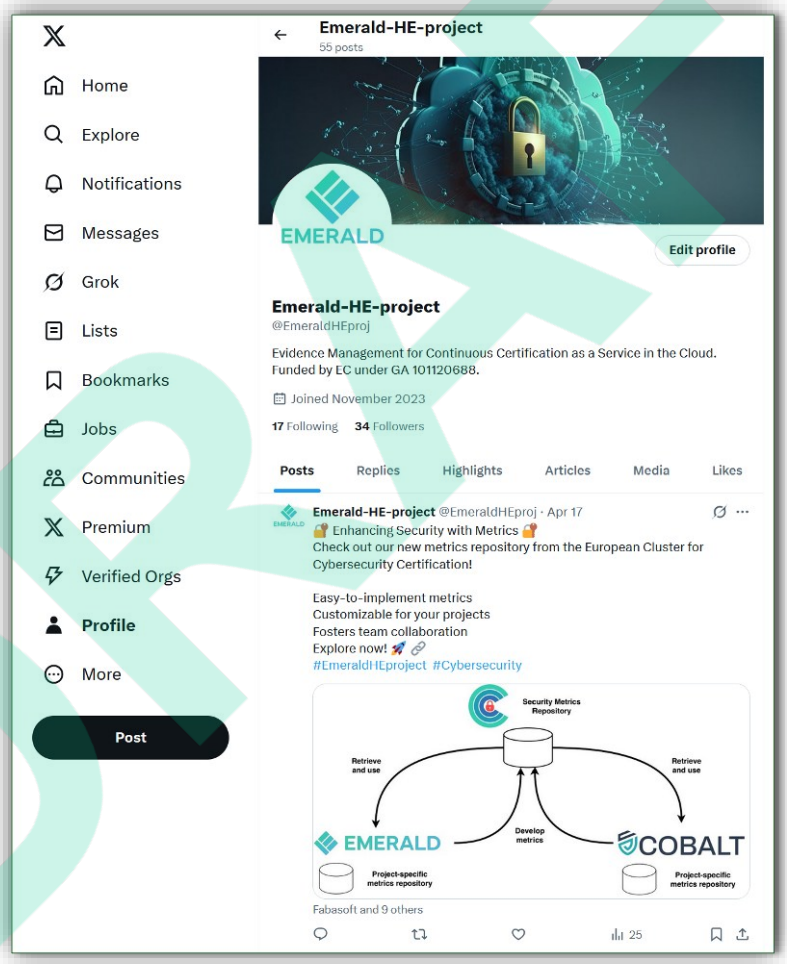


Figure 12. Homepage of the X account of EMERALD

3.2.2 LinkedIn

LinkedIn (see Figure 13) became the main social media platform for EMERALD, supporting the communication of project achievements and engagement with professionals and organisations working in cybersecurity, cloud computing, and certification. The platform was also used to

CC BY-SA

promote EMERALD fragments (see Section 3.1.2), encouraging users to access more detailed information through direct links.

As of October 2026, the EMERALD LinkedIn page had reached 132 followers. During the preceding 12 months, 42 posts were published, generating 9,685 impressions and 362 reactions (see Figure 14). **These results demonstrate the platform's contribution to increasing the visibility of EMERALD and encouraging engagement with project-related content.** The LinkedIn page is available at the following link: https://www.linkedin.com/company/emerald-he-project/.

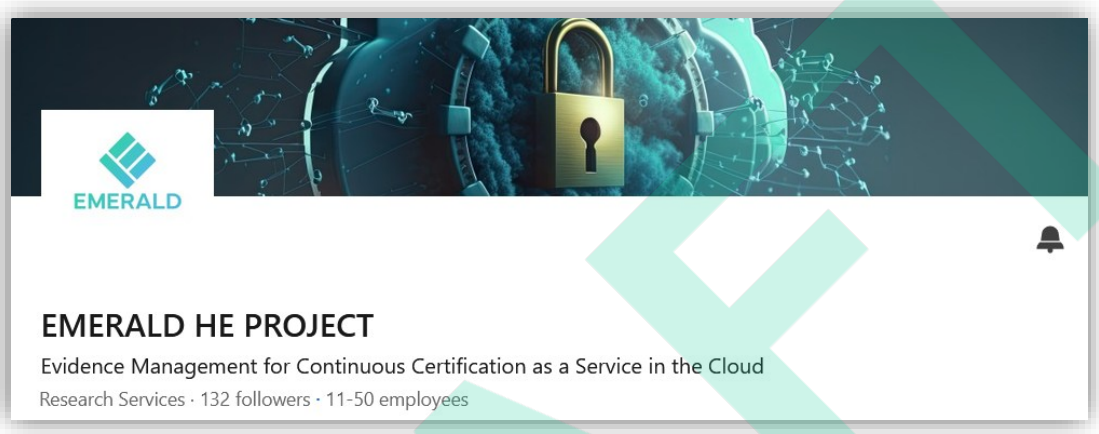


Figure 13. Homepage of the LinkedIn page of EMERALD



Figure 14. Analytics for the LinkedIn page of EMERALD over the past 365 days

Overall, LinkedIn proved to be an effective communication channel, particularly in terms of publication frequency and engagement. **The results achieved exceeded the initial objectives established for this platform,** confirming its suitability for communicating EMERALD's activities and results to professional audiences.

3.2.3 YouTube

The EMERALD YouTube channel (see Figure 15) was established in April 2024 as a dedicated platform for hosting and sharing video content related to the project, its technological developments, and its main results. Unlike LinkedIn, which was primarily used to promote updates and direct visitors to the project website, YouTube served as a repository for audiovisual materials, allowing interested audiences to access presentations and demonstrations of EMERALD solutions.

During the first reporting period, two videos were published: an introductory video produced by TECNALIA, presenting the project's objectives and approach to evidence management for continuous cloud certification, and a second video developed by SCCH, illustrating its

(cc) BY-SA

contribution to the project. Further details on these initial videos are provided in the previous version of the Dissemination and Communication Report [2].

During the second reporting period, eight additional videos were produced to illustrate the EMERALD framework and its practical applications. The first video provides an overview of the framework's architecture and core functionalities. Four videos present mock-ups developed as part of the UI/UX design activities, illustrating user interactions related to Certification Schemes, Targets of Evaluation, and Audit Scopes, with the latter divided into setup and management. The remaining three videos demonstrate the actual implementation of these same functional streams within the EMERALD CaaS solution. Together, these videos support stakeholder understanding and contribute to the dissemination of the project's results. They are described in greater detail in Section 4.4.

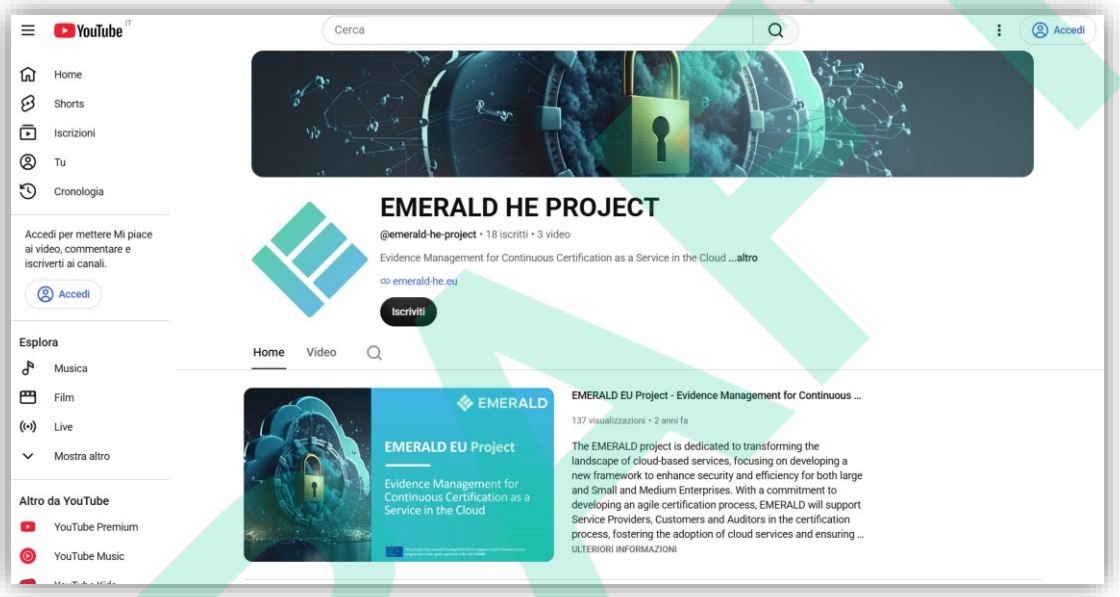


Figure 15. Homepage of the YouTube channel of EMERALD

To maximise their visibility, the videos were promoted through the project's communication channels, particularly LinkedIn and the EMERALD website, allowing interested stakeholders to access the content and explore the developed solutions. The EMERALD YouTube channel is available at https://www.youtube.com/@emerald-he-project.

3.3 Flyers

The EMERALD flyers have been produced with the aim of **raising awareness** of the EMERALD project and **presenting key project information and main results in a straightforward manner.** They also aim to highlight the project's innovative approach to evidence management for continuous certification of cloud services and to encourage readers to visit EMERALD's website for further information.

The format adopted for the three flyers produced during the project is a **tri-fold layout, carefully designed to combine aesthetic appeal with clarity of content.** Each of its six panels serves a distinct purpose, guiding the reader through a comprehensive overview of the project. The layout maintains a balanced integration of textual content and visual elements, ensuring a cohesive appearance while making the information accessible and easy to understand.

CC BY-SA

Following the production of the first flyer by CNR during the first reporting period, as documented in deliverable D6.1 [4], **two additional flyers were developed during the second reporting period.** The second flyer[11], completed in October 2025 by TECNALIA and CNR, presented the main project milestones, highlighting the progress achieved, key technical developments, and the release of the first integrated EMERALD solution, including an overview of its architecture and functionalities. The third and final flyer[12] was produced towards the end of the project by Fabasoft and CNR, providing a summary of the main results and impact achieved, with a particular focus on the pilot activities and the validation of the EMERALD framework in real-world scenarios.

All flyers can be downloaded on the EMERALD website[13]. The second and third flyers are also included in *APPENDIX A*.

3.4 Press releases

The EMERALD press releases aimed to **highlight the project's key milestones** by providing a clear and concise overview of its objectives, major achievements, adopted approaches, and benefits. They represented an essential communication tool for maintaining project visibility and engaging with a broad and diverse audience.

During the first reporting period, an initial press release was published by the consortium in February 2024 and translated into the official languages of the project partners. In addition, two press releases were produced independently by SCCH and CaixaBank for dissemination through national and local media. Further details on these activities are provided in the previous version of the Dissemination and Communication Report [2].

During the second reporting period, a second and final press release was produced in October 2026, presenting the project's main achievements and results. Originally written in English, it was subsequently translated into the languages of the participating partners, namely Finnish, German, Italian, Polish, and Spanish. The final press release and its translations are included in *APPENDIX B*.

The press releases were disseminated through the project's social media channels and made available for download in all language versions on the EMERALD website (see Figure 16), under the “Communication” section[14].

[11] https://www.emerald-he.eu/flyers/#flipbook-df_3770/1/
[12] https://www.emerald-he.eu/flyers/#flipbook-df_4054/1/
[13] https://www.emerald-he.eu/flyers/
[14] https://www.emerald-he.eu/press-release/

(cc) BY-SA

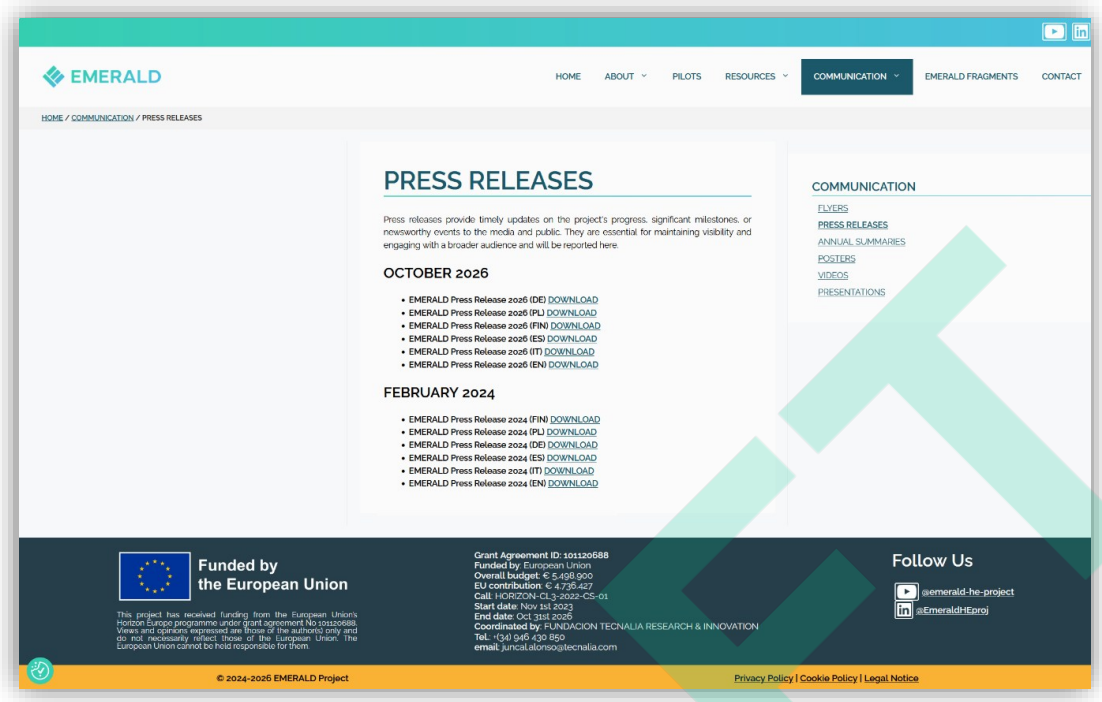


Figure 16. Webpage dedicated to press releases on the EMERALD website

DRAFT

CC BY-SA

4 Dissemination Activities

This section reports on the dissemination activities carried out during the second eighteen-month period of the EMERALD project. It builds upon the results presented in the previous version of the Dissemination and Communication Report deliverable [2], extending the overview of dissemination efforts and their outcomes over the reporting period. The revision of the dissemination KPIs can be found in Section 6.

Dissemination activities mainly include scientific publications, participation in industrial events related to EMERALD's topics, as well as contributions to conferences, panels, lectures, seminars, and similar venues where the EMERALD project and its results have been presented.

These activities are supported by a set of dedicated dissemination materials specifically created for the EMERALD project, which include brochures, flyers, posters, showcases, and presentations, all designed to effectively disseminate the project's objectives, results, and expected impact to a wide range of stakeholders.

4.1 Publications

During the first 18 months of the EMERALD project, a total of five scientific publications were produced, including one journal paper and four conference contributions. Further details of these publications are provided in the previous version of the Dissemination and Communication Report [2].

From M19 to M36, the consortium produced **9 additional scientific publications**, **all of which are conference contributions**. These publications are listed in Table 2.

DRAFT

CC BY-SA

Table 2. List of scientific publications produced in the second reporting period

Status	Title of the article	Authors and Organisations	Title of the journal or proceedings	Volume, number, pages	Publisher	Year	Identifier (if available)	Open access provided?
Published	Efficient Software Security Evaluation: A Human-in-the-Loop Approach (Best Paper)	Christian Banse, Immanuel Kunz, Alexander Küchler, Shala Leutrim, Konrad Weiss, Maximilian Kaul	Proceedings of 10th International Workshop on Testing Extra-Functional Properties and Quality Characteristics of Software Systems (ITEQS 2026) @ 2026 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW 2026), 18/05/2026, Daejeon, South Korea	pp. 139-148	IEEE Digital Library (IEEE Xplore)	2026	https://doi.org/10.1109/ICSTW72326.2026.00037	An open-access version will be available shortly
Published	Developing Security Metrics for Automated Compliance Checking	Immanuel Kunz, Nico Haas, Angelika Schneider and Christian Banse	Proceedings of ICT Systems Security and Privacy Protection (IFIP-SEC 2026). Advances in Information and Communication Technology (IFIP-SEC 2026), 9-11/06/2026, Perth, Australia	Vol. 787, pp. 288-301	Springer	2026	https://doi.org/10.1007/978-3-032-27993-4_20 https://doi.org/10.48550/arXiv.2610.32690 (arXiv version)	Yes
Published	Automatic Association of Cloud Security Controls and Quantifiable Metrics for Certification	John Bianchi, Shuya Dong, Luca Petrillo, Marinella Petrocchi	2nd Workshop on Whole-Lifecycle Security for Smart Systems Methods and Tools (LIFESEC 2026) @ 12th IEEE International Conference on Smart Computing (SmartComp 2026), 22/06/2026, Messina, Italy	pp. 73-78	IEEE Digital Library (IEEE Xplore)	2026	https://doi.org/10.1109/SmartComp-Companion70724.2026.00029 https://doi.org/10.48550/arXiv.2503.09460 (arXiv version)	Yes
Accepted, in press	Automated Compliance Mapping in Cloud Security with Domain-Adapted Sentence Transformers	John Bianchi, Luca Petrillo, Fabio Martinelli, Marinella Petrocchi	30th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2026), 09-11/09/2026, Dublin, Ireland	In press	Elsevier	2026	https://doi.org/10.48550/arXiv.2607.06364 (arXiv version)	Yes

(cc) BY-SA

Status	Title of the article	Authors and Organisations	Title of the journal or proceedings	Volume, number, pages	Publisher	Year	Identifier (if available)	Open access provided?
Accepted, in press	Securing the Seas: Privacy-Enhancing Technologies and Human-Machine Interaction in Maritime Cloud Environments	Daisy Romanini, Marinella Petrocchi (CNR), Fabio Pinelli, Fabio Martinelli, S. Vujicic	Proceeding of 26th Annual General Assembly – Human Centered Digital Ocean: Educating safe & green global maritime professionals (IAMU AGA 2026), 07-10/10/2026, Split, Croatia	In press	International Association of Maritime Universities (IAMU)	2026	Proceedings of the International Association of the Maritime Universities (IAMU) Conference	Yes
Accepted, in press	Revocable ABE protocol for Blockchain auditing systems with SSI	Xabier Barguilla, Cristina Regueiro, Oscar Lage and Jasone Astorga (TECNALIA)	Proceeding of 8th International Congress on Blockchain and Applications (BLOCKCHAIN'26), 21-23/10/2026, Naples, Italy	In press	Springer	2026	https://scienceportal.tecnalia.com/files/77306263/BLOCKCHAIN_26_Workshop.pdf	Yes
Accepted, in press	Towards Context-Aware Ontology Extension from Operational Metrics	Hussain Hussain (SCCH), Stefan Schöberl (SCCH), Angelika Schneider (FHG), Verena Geist (SCCH)	Proceeding of the 18th International Conference on Knowledge Engineering and Ontology Development (KEOD 2026), 29-30/10/2026, Angers, France	In press	SCITEPRESS	2026	https://doi.org/10.48550/arXiv.2607.29553 (arXiv version)	Yes
Accepted, in press	Beyond Static Audits: Using OSCAL to Streamline Continuous Cybersecurity Certification	I. Koufos (NCSRD), S. Matheu (UMU), I. Etxaniz Errazkin, A. Molinuevo Martin, A. Gento Manzano (TECNALIA), G. Xilouris, M.-A. Kourtis (NCSRD), A. Skarmeta (UMU)	ETSI Security Conference 2026, Sophia Antipolis, France, 19-22/10/2026	In press	ETSI	2026	https://dsp.tecnalia.com/bitstreams/2b441067-b763-40a3-8133-18a6ef5fb3f9/download	Yes
Accepted, in press	DEMO: Towards Compliance Monitoring Across All Layers of Heterogeneous Software Products with CONFIRMATE	Andreas M. Binder, Christian Banse, Leutrim Shala, Alexander Küchler, Immanuel Kunz, Maximilian Kaul, Konrad Weiss (FhG)	Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS 2026) – Demo Track, 15-19/11/2026, The Hague, Netherlands	In press	ACM	2026	In press	Not yet

(cc) BY-SA

4.2 EMERALD News

EMERALD News consists of annual summaries that provide an accessible and comprehensive overview of the project's progress, achievements, and key findings. These summaries are designed to engage a broad audience, including stakeholders, funding bodies, and the public, by highlighting milestones and future directions. They are distributed through the project's website, emails, and social media channels to ensure widespread dissemination.

The EMERALD annual summaries are designed as A5 booklets in landscape orientation, suitable for both digital reading and printing. They follow a common structure and visual identity, presenting the project, its consortium and work packages, the main activities and achievements of the corresponding year, and the next steps of the project.

The first EMERALD Annual Summary, produced in M12, presented the progress and results achieved during the first year of the project. A detailed description of its structure and contents is provided in the previous version of the Dissemination and Communication Report [2].

The second EMERALD Annual Summary[15] was produced at the end of the second year of the project. Building on the first edition, it provides **an updated overview of the progress and results achieved during the second year**. In particular, it highlights the advancement and integration of the technical components, improvements to the underlying architecture, and developments in evidence extraction, metric evaluation, and trust mechanisms. It also reports on the iterative design, co-creation, and usability testing of the EMERALD User Interface. Furthermore, the summary describes the expansion and validation of pilot activities in public and hybrid cloud-edge environments and reports on the progress of dissemination, standardization, and exploitation activities. Overall, the second edition reflected **the transition of EMERALD from component development** and prototype **validation towards the integration of a fully operational Compliance-as-a-Service** solution.

The third and final EMERALD Annual Summary[16] was produced towards the end of the project, providing an overview of the main results and achievements of the third year. Particular attention was given to the **pilot activities and the validation of the EMERALD framework**, which played a central role during the final year. The summary presents the application and validation of the developed solutions within the pilot environments, including the audit activities, while also highlighting the main technical developments and achievements reached during the final year of the project.

Screenshots of the last two annual summaries are provided in *APPENDIX C*. The published editions are also available on the EMERALD website[17].

4.3 Posters

During the first 18 months of the project, three posters were produced to enhance the visibility of EMERALD and support the dissemination of project activities and results at relevant events and conferences. Two of them provided a general overview of the project and its achievements, while the third supported the presentation of specific research results. Further details on these posters are provided in the previous version of the Dissemination and Communication Report [2].

[15] https://www.emerald-he.eu/annual-summaries/#flipbook-df_3915/1/
[16] https://www.emerald-he.eu/annual-summaries/#flipbook-df_4114/1/
[17] https://www.emerald-he.eu/annual-summaries/

(cc) BY-SA

Between M19 and M36, **one additional scientific poster was produced to support the presentation of the paper "Towards Context-Aware Ontology Extension from Operational Metrics"** at the 18th International Conference on Knowledge Engineering and Ontology Development (KEOD 2026). This poster contributed to the dissemination of EMERALD's scientific results within the research community, and it is included in *APPENDIX D*.

Overall, four posters were produced during the project, exceeding the corresponding KPI target, which had already been achieved during the first reporting period. In parallel, as the project progressed towards the integration, validation, and demonstration of its results, dissemination activities increasingly focused on other formats, including project showcases, presentations, and annual summaries, which were better suited to highlighting the evolving project results and demonstrating the functionalities and practical applications of the EMERALD framework.

4.4 Project showcases

Videos represent an effective tool for communicating and disseminating the activities, achievements, and results of the EMERALD project, enabling both technical and non-technical audiences to better understand the developed solutions and their practical applications.

During the first 18 months of the project, two videos were produced to introduce EMERALD and support its communication and dissemination activities. These materials were described in the previous version of the Dissemination and Communication Report (D6.4) [2].

Between M19 and M36, **eight additional videos were produced**, focusing on the EMERALD framework, its main functionalities, and its practical applications. In particular, these included:

- **One overview video** introducing the EMERALD framework, its overall architecture, main components, and key functionalities, providing an accessible introduction to the developed solution.
- **Four UI/UX mock-up videos** developed as part of the interface design activities, illustrating the envisioned user interactions and workflows related to Certification Schemes, Targets of Evaluation, and Audit Scopes, with the latter divided into audit scope setup and management.
- **Three technical demonstration videos** showing the actual implementation of the three main functional streams of the EMERALD Compliance-as-a-Service (CaaS) solution: Certification Schemes, Targets of Evaluation, and Audit Scopes.

These additional videos were designed to provide a more detailed understanding of the EMERALD framework and its capabilities, **illustrate the evolution from UI/UX design to functional implementation**, demonstrate the practical application of the developed technologies, and facilitate knowledge transfer to relevant stakeholders, including researchers, industry representatives, potential adopters, and the wider community.

The mock-up videos illustrate the interface design and intended user experience, while the technical demonstration videos show the corresponding functionalities implemented within the EMERALD framework. The latter were produced using screen recordings of the framework in operation, complemented by synthetic voice narration (Text-to-Speech), providing step-by-step explanations of the actions performed and the functionalities demonstrated.

Overall, **ten videos were produced throughout the project**, contributing to the visibility of EMERALD and supporting the dissemination and exploitation of its results. All project showcases

(cc) BY-SA

and videos are available both on the EMERALD website[18] and on the EMERALD YouTube channel[19].

4.5 Events

Participation in relevant events represented an important dissemination activity for EMERALD, contributing to increasing the project's visibility, fostering exchanges and collaboration with other initiatives, and engaging with relevant research and industrial communities. As in the previous reporting period, a distinction is made between **active participation**, where EMERALD or project-related results were presented or discussed as part of the event programme, and **simple attendance**, where partners participated in events relevant to the project without directly presenting EMERALD.

During the first 18 months of the project, EMERALD partners participated in a variety of events through talks, paper and poster presentations, webinars, seminars, a booth, and a keynote speech. A detailed overview of these activities is provided in the previous version of the Dissemination and Communication Report [2].

Between M19 and M36, dissemination through events continued, with particular emphasis on **the presentation of scientific results produced within the project at international conferences and workshops**. These activities included presentations of EMERALD-related papers at venues such as IFIP SEC 2026, ITEQS 2026, IEEE SmartComp 2026, BLOCKCHAIN 2026 and KEOD 2026, alongside participation in other scientific, industrial, and collaborative events relevant to the project's objectives. As the project approached its final stages, events also provided opportunities to present and discuss the more mature results of the EMERALD framework and its application and validation activities.

The events in which EMERALD was actively presented during the second reporting period, together with information on the type of activity, location, date, target audience, and estimated audience size, are listed in Table 3. Events attended by project partners without a direct presentation of EMERALD or its results are reported separately in Table 4.

[18] https://www.emerald-he.eu/videos/
[19] https://www.youtube.com/@emerald-he-project

(cc) BY-SA

Table 3. List of events in which the EMERALD project (or parts of it) has been actively presented

Event	Date	Name and type of audience	Countries addressed	Size of audience	EMERALD People attending (names)
Webinar: "Innovation in Action: Strategies for Exploiting Horizon Europe Results"	Jun 23, 2025	Horizon Europe projects and exploitation stakeholders	Europe	50	Juncal Alonso, Cristina Martinez (TECNALIA), Björn Fanta (FABAR)
Panel participation: "ETSI Security Conference 2025"	Oct 5-10, 2025	Standardization and security experts	Europe	250+	Björn Fanta (FABAR)
Webinar: "European Blockchain Sandbox – Launch of the Third Cohort Best Practices Report" https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox-releases-third-cohort-best-practices-report en emerald	Feb 11, 2026	European Blockchain Sandbox participants, regulators and interested public	Europe	n.a.	Cristina Martinez, Cristina Regueiro (TECNALIA)
Webinar&Roundtable: "Policy and Certification for a Trusted IoT Ecosystem in the EU" Global IoT Day 2026, online https://iotday.org/events/2025/global-iot-day-webinar-and-roundtable-policy-certification-for-a-trusted-iot-ecosystem-in-the-eu/	Apr 09, 2026	Horizon Europe projects and stakeholders working on IoT security, policy and certification	Europe (online)	50	Björn Fanta (FABAR), Nico Haas (FHG), Michela Fazzolari (CNR)
Paper presentation: "Efficient Software Security Evaluation: A Human-in-the-Loop Approach" at ITEQS 2026 @ ICST 2026, Daejeon, South Korea	May 18, 2026	Academia	International	30	Christian Banse (FHG)
Paper presentation: "Developing Security Metrics for Automated Compliance Checking" at 41st IFIP TC11 Information Security & Privacy Conference (IFIP SEC 2026), Perth, Australia	Jun 09-11, 2026	Academia	International	70	Christian Banse (FHG)

DRAFT

(cc) BY-SA

Event	Date	Name and type of audience	Countries addressed	Size of audience	EMERALD People attending (names)
Paper presentation: "Automatic Association of Cloud Security Controls and Quantifiable Metrics for Certification" at 2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools – LIFESEC 2026, co-located with IEEE SmartComp 2026	Jun 22-25, 2026	Academia	International	40	John Bianchi (CNR)
Paper presentation: "Automated Compliance Mapping in Cloud Security with Domain-Adapted Sentence Transformers" at 30th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2026), Dublin, Ireland	Sep 09-11, 2026	Academia	International	200	Luca Petrillo (CNR)
Keynote presentation: "Elastic Kubernetes Needs a Home: Why Infrastructure Is Key" at Edgecase 2026, Hilversum, Netherlands	Sep 24, 2026	Cloud infrastructure professionals, Kubernetes practitioners, academia, industry	Europe	40	Constantino Vázquez (ONS)
Webinar: "EC3 Project Webinar – From Research to Results", online	Oct 07, 2026	Horizon Europe project representatives, cybersecurity researchers, cloud security and certification professionals, industry stakeholders	Europe	50	Cristina Martinez, Juncal Alonso (TECNALIA), Björn Fanta (FABAR), Michela Fazzolari (CNR)
Paper presentation: "Securing the Seas: Privacy-Enhancing Technologies and Human-Machine Interaction in Maritime Cloud Environments" at IAMUC 2026 – IAMU AGA26, Split, Croatia	Oct 08-09, 2026	Academia	International	150	Daisy Romanini (CNR)
Paper presentation: "Revocable ABE Protocol for Blockchain Auditing Systems with SSI" at 8th International Congress on Blockchain and Applications (BLOCKCHAIN'26), Naples, Italy	Oct 21-23, 2026	Academia	International	100	Xabier Barguilla (TECNALIA)

DRAFT

(cc) BY-SA

Event	Date	Name and type of audience	Countries addressed	Size of audience	EMERALD People attending (names)
Panel participation: “Certifying the Future: A Live Research Debate on Security Certification” at ETSI Security Conference 2026, Sophia Antipolis, France	Oct 22, 2026	International cybersecurity and standardisation experts from industry, government organisations, standards bodies, academia and EU research projects	International	250	Björn Fanta (FABAR)
Poster presentation: "Towards Context-Aware Ontology Extension from Operational Metrics" at the 18th International Conference on Knowledge Engineering and Ontology Development (KEOD 2026), Angers, France	Oct 28-30, 2026	Academia	International	100	Hussain Hussain (SCCH)

DRAFT

(cc) BY-SA

Table 4. List of the events attended by partners, whose topics are EMERALD-related.

Event	Date	Name and type of audience	Countries addressed	Size of audience	EMERALD People attending (names)
NexusForum 2025	Nov 5-6, 2025	EU projects, industry, policymakers and researchers working on AI, Cloud/Edge and sustainability	Europe	200	Netsanet Haile Gebreyesus, Julius Holderer (IONOS), Björn Fanta (FABAR)
CSC Cybersecurity Standardisation Conference 2026	Mar 12, 2026	European cybersecurity and standardization community	Europe	180	Björn Fanta (FABAR)
2026 European Cybersecurity Certification Conference	Apr 15, 2026	European cybersecurity-certification community	Europe (Cyprus and online)	200	Björn Fanta (FABAR), Michela Fazzolari (CNR)

4.6 Presentations

Presentations represented an important tool for disseminating EMERALD's objectives, progress, and results to scientific, industrial, and other relevant stakeholders, supporting knowledge exchange and engagement with the wider community.

During the first 18 months of the project, a general EMERALD presentation was developed to provide partners with a common resource for introducing the project at events and meetings. Further details are provided in the previous version of the Dissemination and Communication Report [2].

During the second reporting period, three additional presentations were developed, focusing on specific aspects of the project and its technological solutions.

The first presentation, entitled **EMERALD Blockchain-based Trustworthiness System**[20] (Figure 17), was delivered by TECNALIA in July 2025 as part of the third cohort of the European Blockchain Sandbox. It focused on the blockchain-based Trustworthiness System (TWS) developed within EMERALD, illustrating its architecture, operation, and role in ensuring the integrity and traceability of evidence used in cloud cybersecurity certification processes.

[20] https://www.emerald-he.eu/wp-content/uploads/2025/12/EMERALD_TWS_Blockchain_Sandbox.pdf

(cc) BY-SA



Figure 17. First slide of the presentation "EMERALD Blockchain-based Trustworthiness System"

The second presentation, entitled **Cybersecurity Certification for the Computing Continuum: Future Challenges and Opportunities**[21] (Figure 18), was delivered by Juncal Alonso, from TECNALIA, in October 2025 at the University of Murcia, as part of its Master's programme in Cybersecurity. It addressed the challenges of cybersecurity certification across the computing continuum and presented the EMERALD approach, objectives, technical components, and Compliance-as-a-Service workflow.



Figure 18. First slide of the presentation "Cybersecurity Certification for the Computing Continuum: Future Challenges and Opportunities"

The third presentation entitled **OSCAL in the EMERALD EU Project** (see Figure 19), delivered on 29 July 2026, provided an overview of the adoption and integration of OSCAL within EMERALD, highlighting its role in supporting standardised, machine-readable compliance information and automated cybersecurity assessment.

[21] https://www.emerald-he.eu/wp-content/uploads/2025/10/UM_TALK_public.pdf

CC BY-SA



Figure 19. First slide of the presentation "OSCAL in the EMERALD EU Project"

In addition, the **EMERALD General Presentation**[22] was updated during the second reporting period to reflect the project's technical progress and latest achievements. The updated version provides a more comprehensive overview of the EMERALD framework, its main components, and its Compliance-as-a-Service approach, ensuring that project partners have an up-to-date and consistent resource for presenting EMERALD to different audiences. A selection of slides from this presentation, focusing on the project's main results and achievements, was used for the EC3 Project Webinar "From Research to Results", held on 7 October 2026.

All four presentations are available on the EMERALD website[23]. The updated General Presentation is also included in *APPENDIX E*.

4.7 Cloud Community Publications

The EMERALD project has gained visibility within the broader scientific and industrial communities through references on external websites, publications, and platforms related to European research initiatives. During the first 18 months of the project, several mentions were identified and documented in the Dissemination and Communication Report – v1 [2]. During the second reporting period, additional references further contributed to increasing the project's visibility and highlighting its involvement in collaborative initiatives and activities related to cybersecurity and cloud certification. These new mentions are presented below.

Webinar "Innovation in Action: Strategies for Exploiting Horizon Europe Results"

EMERALD was featured on the European Cluster for Cybersecurity Certification (EC3) website as one of the projects jointly organising the **webinar "Innovation in Action: Strategies for Exploiting Horizon Europe Results",** held on 23 June 2025. The event brought together the TELEMETRY, EMERALD, COBALT, and DOSS projects to share experiences, discuss common challenges, and explore effective strategies for maximising the exploitation and impact of research results. The webinar also provided an opportunity to exchange knowledge and strengthen collaboration among European cybersecurity research initiatives (https://cybersecuritycertcluster.eu/#Events).

[22] https://www.emerald-he.eu/wp-content/uploads/2026/07/EMERALD_Presentation_v2.0_draft.pdf
[23] https://www.emerald-he.eu/presentations/

(cc) BY-SA

EU Projects Joint Workshop on Exploitation & Technical Collaboration

EMERALD was featured on the COBALT project website as one of the four Horizon Europe projects participating in the **Joint Workshop on Exploitation & Technical Collaboration**, held on 20 November 2025 in Rome, Italy, and hosted by Engineering Group. The workshop brought together EMERALD, COBALT, DOSS, and TELEMETRY to exchange experiences, present their technical approaches, and explore synergies in cybersecurity and certification. Discussions focused on identifying opportunities for technical collaboration, aligning exploitation strategies, and defining potential joint activities to maximise the impact and long-term sustainability of project results (https://horizon-cobalt.eu/cobalt-participates-in-eu-projects-joint-workshop-on-exploitation-technical-collaboration/).

Global IoT Day Webinar and Roundtable 2026

EMERALD participated in the Global IoT Day Live Webinar and Roundtable, held on April 9, 2026. The event focused on policy and certification approaches for building a secure and trusted IoT ecosystem. EMERALD contributed alongside the COBALT project with a presentation entitled "Developing Common Security Metrics for Continuous Certification", delivered by Immanuel Kunz and Christian Banse from Fraunhofer AISEC, highlighting approaches to supporting continuous cybersecurity certification (https://dossproject.eu/global-iot-day-webinar-and-roundtable-2026/).

LIFESEC 2026 – Workshop on Whole-Lifecycle Security for Smart Systems

EMERALD was mentioned on the TELEMETRY project website as one of the six Horizon Europe projects jointly organising the 2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools (LIFESEC 2026), held on 22 June 2026 in Messina, Italy, as part of IEEE SmartComp 2026. The workshop brought together researchers and practitioners to discuss cybersecurity certification, compliance, IoT security, and other challenges related to whole-lifecycle security. The event provided an opportunity to exchange knowledge and strengthen collaboration among European research initiatives (https://telemetry-project.eu/lifesec-2026-sparks-discussion-on-whole-lifecycle-security/).

Cross-Project Exploitation Workshop

EMERALD was featured on the COcyber project website as one of the European cybersecurity projects participating in the Cross-Project Exploitation Workshop, held on 18 June 2026. The workshop brought together Horizon Europe and Digital Europe projects to exchange experiences, discuss exploitation strategies, and explore opportunities for collaboration and the uptake of project results.

Discussions focused on Key Exploitable Results (KERs), intellectual property management, potential exploitation pathways, and sustainability strategies, helping participating projects identify common challenges and opportunities for synergies (https://cocyber.eu/article-news/cocyber-hosts-cross-project-exploitation-workshop-he-and-digital-europe-cybersecurity, https://telemetry-project.eu/telemetry-presents-its-exploitation-approach-at-cross-project-workshop/).

EC3 Project Webinar – From Research to Results

EMERALD was featured on the European Cluster for Cybersecurity Certification (EC3) and TELEMETRY project websites as one of the four Horizon Europe projects jointly organising the final EC3 Project Webinar, held on 7 October 2026. The event brought together EMERALD, COBALT, DOSS, and TELEMETRY to present their respective approaches, key results, and

(cc) BY-SA

achievements in cybersecurity research and innovation. The webinar provided an opportunity to share the outcomes of the four projects with a wider audience, highlight their contributions to cybersecurity certification and related challenges, and promote knowledge exchange among European research initiatives (https://cybersecuritycertcluster.eu/, https://telemetry-project.eu/category/events/).

ETSI Security Conference 2026 – Panel "Certifying the Future: A Live Research Debate on Security Certification"

EMERALD was featured on the ETSI Security Conference 2026 website as one of the European research projects participating in the panel "Certifying the Future: A Live Research Debate on Security Certification", held on 22 October 2026 in Sophia Antipolis, France. The panel brought together representatives from EMERALD, TELEMETRY, CUSTODES, COBALT, and OSCRAT to discuss current approaches to cybersecurity certification in the age of artificial intelligence, exploring common perspectives, differences, and future challenges (https://www.etsi.org/events/2645-etsi-security-conference-oct2026/).

DRAFT

CC BY-SA

5 Networking Activities

Networking and collaboration with other European research projects and initiatives continued to play an important role in EMERALD during the second reporting period. Building on the connections established during the first 18 months, particularly through the European Cluster for Cybersecurity Certification (EC3)[24], the project focused on strengthening existing collaborations, promoting knowledge exchange, and identifying opportunities for joint dissemination, technical cooperation, and exploitation of research results.

These networking activities focused on four main areas: technological collaborations, co-organised events, joint dissemination, and participation in working groups. Technological collaborations included the development of shared resources and exchanges on complementary tools and approaches. Joint events and dissemination initiatives strengthened cooperation among European research projects and supported the exchange and promotion of research results. In parallel, participation in working groups and standardisation-related initiatives, together with the continued engagement of the External Advisory Board, contributed to knowledge exchange and the alignment of EMERALD's developments with broader European efforts in cybersecurity certification.

5.1 European Cluster for Cybersecurity Certification

The EC3, established during the first reporting period, continued to serve as a platform for collaboration among European research and innovation projects addressing the challenges of next-generation agile cybersecurity certification. Its objectives, initial membership, planned activities, and official launch at CLOSER 2025 are described in the Dissemination and Communication Report – v1 [2].

During the second reporting period, the cluster expanded its membership and strengthened its collaborative activities, moving from its initial establishment towards more concrete technical cooperation, joint dissemination, and exploitation initiatives. The cluster brought together nine European research projects: EMERALD, COBALT[25], CERTIFAI[26], CERTIFY[27], DOSS[28], TELEMETRY[29], CONFIRMATE[30], CUSTODES[31], and OSCRAT[32] (see Figure 20). This expansion has broadened the range of expertise represented within EC3, covering cloud and IoT security, continuous certification, conformity assessment, and automated compliance.

[24] https://cybersecuritycertcluster.eu/
[25] https://horizon-cobalt.eu/
[26] https://certifai.info/
[27] https://certify-project.eu/
[28] https://dossproject.eu/
[29] https://telemetry-project.eu/
[30] https://confirmate-project.eu/
[31] https://custodes-project.eu/
[32] https://oscrat.eu/

(cc) BY-SA

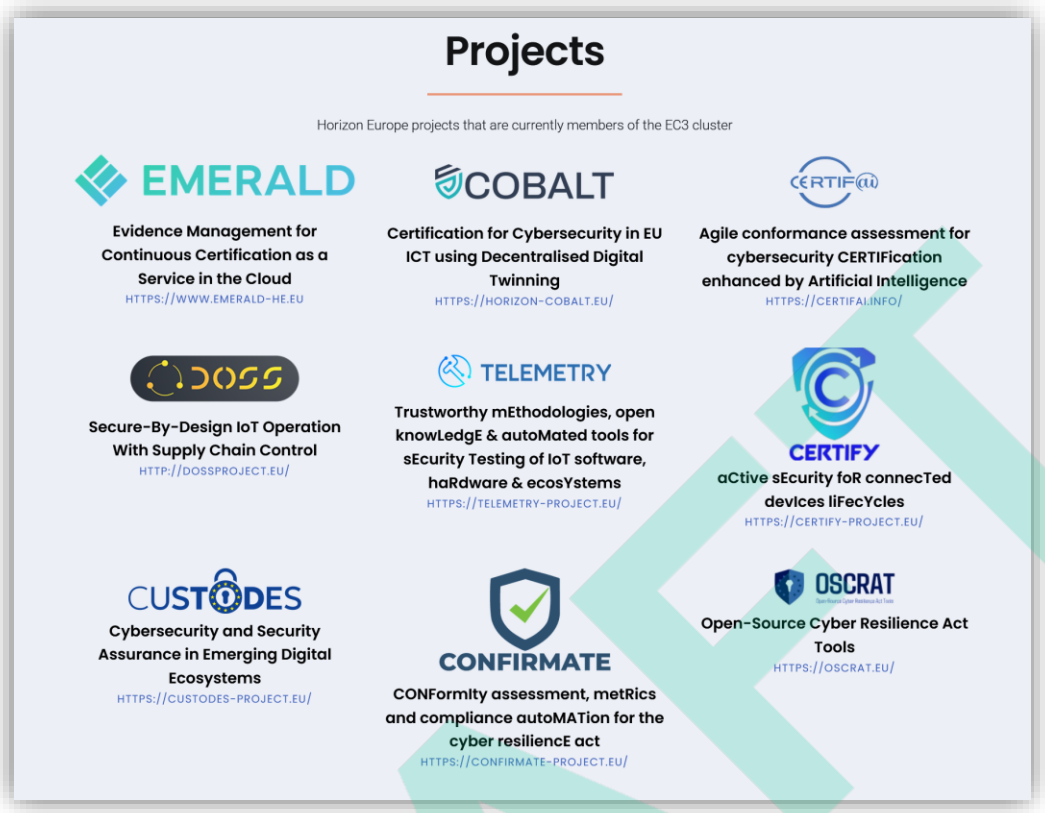


Figure 20. Projects currently involved in the EC3

On the technical side, collaboration progressed through the **Collaborative Metrics Repository (CMR)**[33], a shared, publicly accessible repository developed to facilitate the definition, maintenance, and reuse of security metrics across participating projects. The repository supports a common approach to metric development, reducing duplication of effort and promoting consistency and interoperability among cybersecurity certification solutions. EMERALD contributed to this initiative and integrated the repository into its framework, enabling the reuse of collaboratively maintained metrics for compliance assessment.

The cluster also expanded its activities beyond technical cooperation, organising and participating in joint workshops, webinars, conference sessions, and exploitation-oriented initiatives. These activities provided opportunities to exchange research findings, discuss common technical and regulatory challenges, explore synergies among project results, and identify potential pathways for their exploitation. Furthermore, the collaboration between EMERALD and COBALT resulted in **two joint scientific publications**, "Developing Security Metrics for Automated Compliance Checking" and "Beyond Static Audits: Using OSCAL to Streamline Continuous Cybersecurity Certification" (see Section 4.1), demonstrating the concrete outcomes of cross-project research cooperation. Joint dissemination activities also included **blog posts** promoting collaborative initiatives and sharing insights into common challenges and developments in cybersecurity certification. These posts are published on the website of the EC3[34], as shown in Figure 21.

[33] https://github.com/Cybersecurity-Certification-Hub/security-metrics
[34] https://cybersecuritycertcluster.eu/#Blog

CC BY-SA

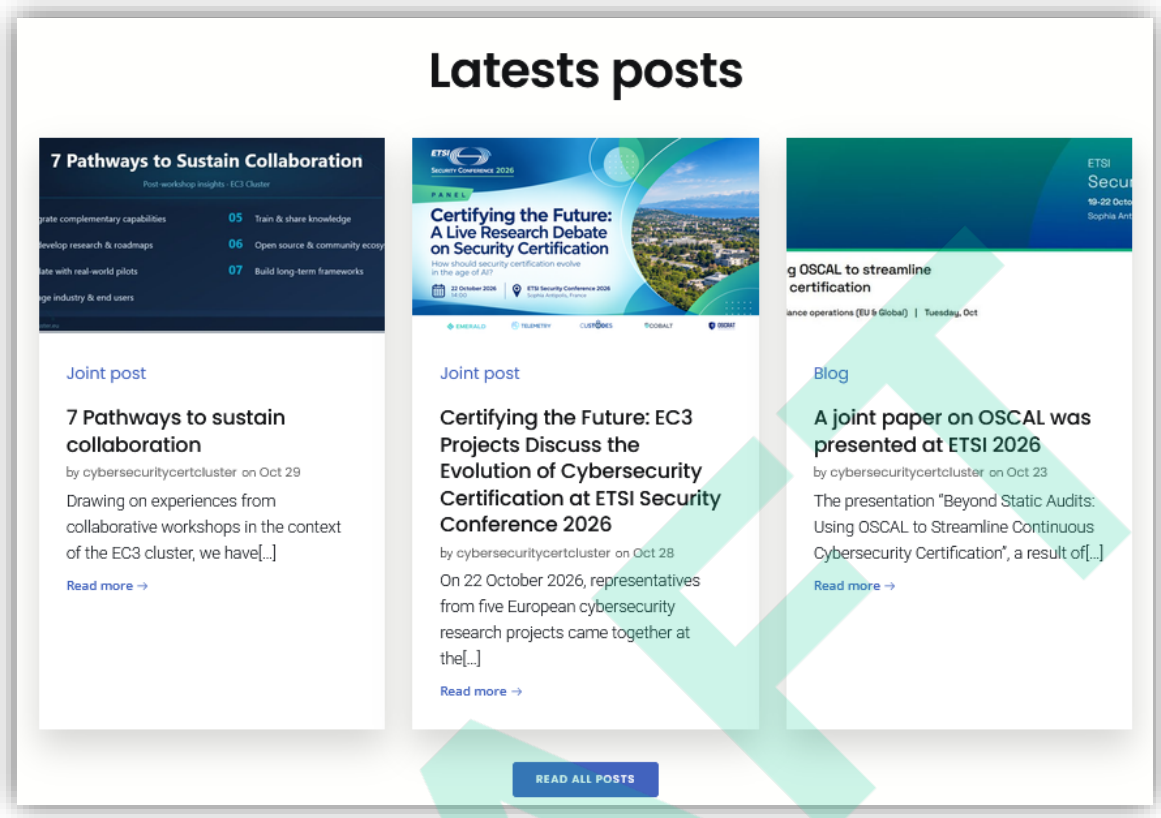


Figure 21. Blog Posts on the EC3 website

In addition, EC3 extended its engagement with the wider cybersecurity community by supporting **EUROSCAL** (The EU Friends of OSCAL)[35], an open community promoting the adoption of machine-readable security requirements and automated compliance approaches based on the OSCAL framework. This initiative complements the cluster's objectives of promoting interoperability and advancing automation in cybersecurity certification.

The main joint activities organised or supported by EC3 during the second reporting period are published in the EC3 website[36] (Figure 22) and described in the following subsections. Additional information on the cluster, its participating projects, and shared resources is available on the EC3 website.

[35] https://euroscal.eu/
[36] https://cybersecuritycertcluster.eu/#Events

CC BY-SA

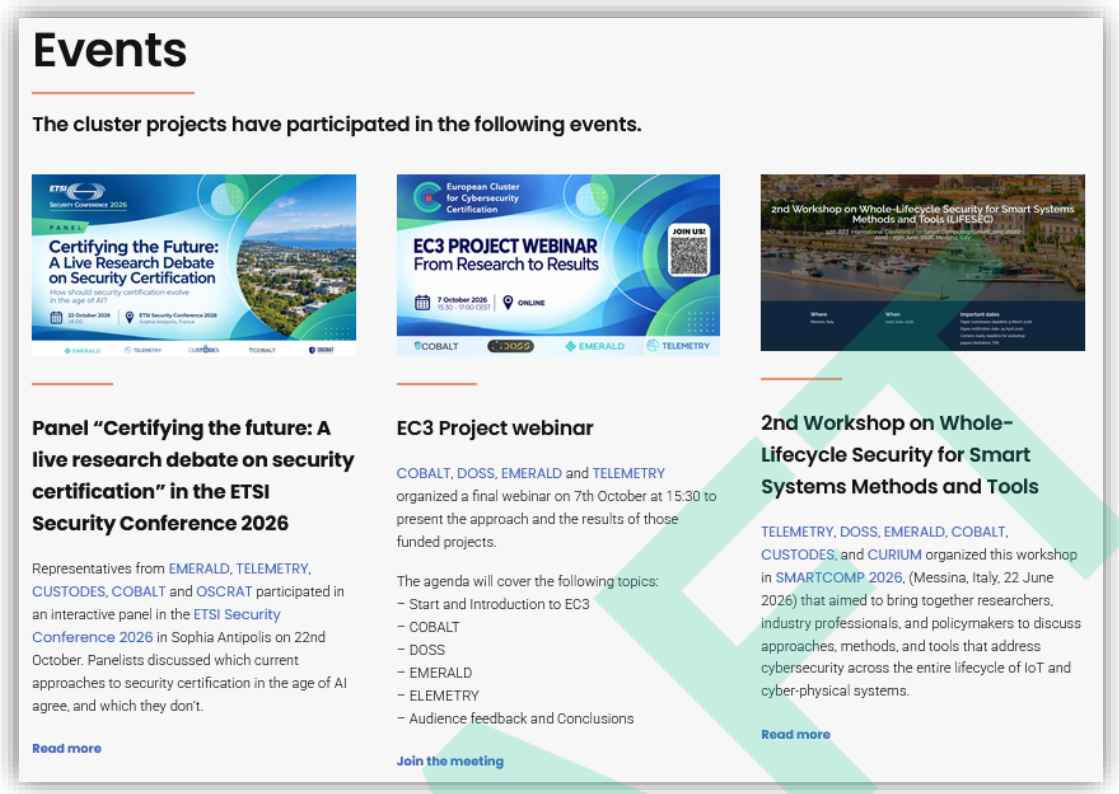


Figure 22. Events on the EC3 website

5.1.1 Webinar "Innovation in Action: Strategies for Exploiting Horizon Europe Results"

On 23 June 2025, the EC3 projects EMERALD, TELEMETRY, COBALT, and DOSS jointly organised the webinar *"Innovation in Action: Strategies for Exploiting Horizon Europe Results*". The event aimed to promote the exchange of experiences and best practices related to the exploitation of research outcomes, bringing together representatives of European cybersecurity projects to discuss common challenges and potential strategies for maximising their impact.

The webinar provided an opportunity for the participating projects to share their approaches to exploitation planning, reflect on the challenges associated with transferring research results towards practical applications, and explore opportunities for collaboration. Particular attention was given to identifying common experiences and potential synergies that could support the long-term sustainability and uptake of project results.

For EMERALD, this initiative contributed to strengthening cooperation within EC3 and exchanging knowledge on exploitation strategies with projects addressing complementary cybersecurity challenges.

CC BY-SA



Figure 23. Promotional graphic for the webinar "Innovation in Action: Strategies for Exploiting Horizon Europe Results"

5.1.2 Joint Exploitation Workshop

On 20 November 2025, the EC3 projects TELEMETRY, COBALT, DOSS, and EMERALD participated in a Joint Exploitation Workshop, hosted by Engineering Group in Rome, Italy. The workshop was organised to strengthen collaboration among the participating projects, exchange practical experiences, and identify complementarities between their technical approaches and exploitation strategies.

The meeting provided a collaborative environment in which project representatives could present their activities, discuss the exploitation potential of their results, and explore opportunities for technical cooperation. Particular attention was given to identifying synergies that could contribute to the sustainability and practical uptake of the solutions developed within the different projects.

The workshop represented an important opportunity to move beyond the exchange of general information towards more focused discussions on potential joint activities. For EMERALD, participation supported the identification of common interests with other EC3 members and contributed to strengthening the collaborative relationships established within the cluster.

DRAFT

CC BY-SA



Figure 24. Participants at the Joint Exploitation Workshop held in Rome on 20 November 2025

5.1.3 Global IoT Day Webinar and Roundtable 2026

On 9 April 2026, EMERALD participated in the "*Global IoT Day Webinar and Roundtable"*, jointly organised with DOSS, COBALT, CUSTODES, and TELEMETRY. The two-hour online event brought together representatives of European research projects to discuss how policy frameworks and cybersecurity certification mechanisms can evolve to support a secure, interoperable, and trusted IoT ecosystem.

The webinar addressed challenges related to cybersecurity certification, regulatory requirements, and the development of approaches capable of supporting security assessment across increasingly complex digital environments. The roundtable format encouraged exchanges among the participating projects, providing an opportunity to compare different perspectives and discuss complementary technological solutions.

EMERALD contributed to the event through the presentation "Developing Common Security Metrics for Continuous Certification", delivered by Immanuel Kunz and Christian Banse from Fraunhofer AISEC. The presentation highlighted approaches to defining and applying measurable security metrics to support continuous cybersecurity certification, contributing to the broader discussion on harmonisation and automation of compliance assessments.



CC BY-SA

Figure 25. Promotional banner for the Global IoT Day Webinar and Roundtable 2026

5.1.4 Cross-Project Exploitation Workshop

On 18 June 2026, EMERALD participated in an online "*Cross-Project Exploitation Workshop"*, organised by the COcyber project[37], bringing together representatives from several Horizon Europe and Digital Europe cybersecurity initiatives, including TELEMETRY, DOSS, CUSTODES, CONFIRMATE, and ENSEMBLE. The workshop aimed to strengthen collaboration among projects and support the transition from research results to practical exploitation.

The event addressed key aspects of exploitation planning, including the management of Key Exploitable Results (KERs), intellectual property rights, ownership arrangements, and compliance with Horizon Europe exploitation requirements. Following an introductory session, participants engaged in interactive breakout discussions to present their project results, identify potential exploitation pathways, and exchange feedback on common challenges, such as stakeholder engagement, access to validation environments, and regulatory complexity.

The workshop also explored opportunities for synergies between projects with complementary objectives. For EMERALD, participation provided an opportunity to exchange experiences on exploitation planning and contribute to discussions on the long-term sustainability and potential uptake of cybersecurity research results.



Figure 26. Screenshot of participants attending the COcyber Cross-Project Exploitation Workshop

5.1.5 2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools (LIFESEC 2026)

On 22 June 2026, EMERALD jointly organised the "*2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools" (LIFESEC 2026)*, held in Messina, Italy, as part of the 12th IEEE International Conference on Smart Computing (SmartComp 2026). The workshop was organised in collaboration with TELEMETRY, DOSS, COBALT, CUSTODES, and CURIUM, building on the first edition held in 2025 and expanding cooperation among European research initiatives.

The workshop aimed to bring together researchers and practitioners to discuss methods and tools for addressing cybersecurity challenges throughout the lifecycle of smart and cyber-physical systems. Its programme included eight research presentations covering topics such as

[37] https://cocyber.eu/

CC BY-SA

cybersecurity certification and compliance, IoT attack detection, vulnerability management, digital twins, and cloud security.

The event encouraged discussions following the presentations. An interactive session dedicated to tools and techniques for whole-lifecycle security also provided opportunities to exchange experiences and collect feedback. For EMERALD, the workshop contributed to strengthening scientific collaboration and promoting exchanges on continuous certification and security assessment within the wider computing continuum.



Figure 27. Promotional banner for the 2nd Workshop on Whole-Lifecycle Security for Smart Systems: Methods and Tools (LIFESEC 2026)

5.1.6 EC3 Project Webinar: From Research to Results

On 7 October 2026, the EC3 projects EMERALD, COBALT, DOSS, and TELEMETRY jointly organised the final "*EC3 Project Webinar: From Research to Results*". The online event aimed to present the approaches, main achievements, and results of the four Horizon Europe projects, providing an opportunity to share their contributions to cybersecurity research and innovation with a wider audience.

The webinar programme opened with an introduction to EC3 and its objectives, followed by dedicated presentations from each participating project. These sessions provided an overview of the different approaches developed to address cybersecurity challenges, highlighting their respective research outcomes and potential applications.

EMERALD contributed through a dedicated presentation of its approach and project results, placing them within the broader context of automated compliance assessment and continuous cybersecurity certification. The webinar concluded with an audience feedback session, encouraging exchanges between participants and project representatives.

Participants identified continuous compliance assessment as the highest-value EMERALD result, closely followed by automated evidence extraction and reusable security metrics and controls. An overwhelming majority (≈93%) rated the results as at least moderately applicable beyond cloud services, signalling strong perceived transferability. Priority application domains concentrated in AI systems across sectors, industrial manufacturing and IoT, and energy and utilities. The principal adoption barrier cited was integration with existing tools and workflows, closely followed by gaining acceptance from auditors and certification bodies, indicating that

(cc) BY-SA

the path to wider deployment depends less on technical capability than on interoperability and regulatory legitimacy.

As one of the final joint dissemination activities of the cluster, the event contributed to showcasing the results of the participating projects and reinforcing the collaborative relationships established through EC3.



Figure 28. Promotional banner for the EC3 Project Webinar "From Research to Results"

5.1.7 ETSI Security Conference 2026 – Panel "Certifying the Future: A Live Research Debate on Security Certification"

As part of the networking and dissemination activities promoted through EC3, representatives of EMERALD, TELEMETRY, CUSTODES, COBALT, and OSCRAT participated in the panel "*Certifying the Future: A Live Research Debate on Security Certification*", organised within the ETSI Security Conference 2026. The session took place on 22 October 2026 in Sophia Antipolis, France, as part of Session D4-4 of the conference programme.

The panel brought together representatives of European research initiatives to discuss current approaches to cybersecurity certification, with particular attention to the challenges introduced by artificial intelligence. The interactive format encouraged debate on areas of agreement and disagreement among the participating projects, providing a forum for exchanging different technical perspectives, certification methodologies, and views on potential future directions.

The session was moderated by Björn Fanta from Fabasoft (FABAR), who also presented the main EMERALD findings in the lightning talk session at the beginning of the panel, alongside Martin Gilje Jaatun from SINTEF (for TELEMETRY) and Yiannis Koufos from NCSRD (for COBALT).

The panel provided an opportunity to share research perspectives with the wider cybersecurity and standardisation community, strengthen cooperation among EC3 members, and contribute to discussions on the future evolution of cybersecurity certification.

CC BY-SA



Figure 29. Promotional banner for the panel "Certifying the Future: A Live Research Debate on Security Certification" at the ETSI Security Conference 2026

5.2 Networking with Other Initiatives

European Telecommunications Standards Institute (ETSI)

EMERALD networks with the European Telecommunications Standards Institute (ETSI) Technical Committees CYBER and SAI through its partner Fabasoft, an active ETSI member. Within this collaboration, EMERALD contributes its research findings on advanced security evidence management, including novel approaches for traceability and automation through *CertGraph*, as well as the use of interoperable formats such as OSCAL (Open Security Controls Assessment Language). These contributions support ongoing standardization efforts around trustworthy cloud certification and AI system assurance, enabling more transparent and efficient assessment processes across Europe. These activities are described in the deliverable D6.7 Exploitation report v2 [3].

EUROSCAL

EMERALD has continued to contribute to Open Security Controls Assessment Language (OSCAL) through collaboration with NIST in different directions: development of technical components compatible with OSCAL, engagement with NIST and participation in several meetings with them and continue leading the EUROSCAL initiative[38]. As reported in D6.7 [3], EMERALD is actively integrating the Open Security Controls Assessment Language (OSCAL) to standardize and automate its cloud compliance processes, thereby fostering seamless interoperability and continuous certification.

HELEN HUB

EMERALD is also featured on the HELEN Hub platform[39], contributing to its visibility within the wider European research and innovation community. This connection provides an additional opportunity for networking and knowledge exchange with other European initiatives.

[38] https://euroscal.eu/
[39] https://www.helen-hub.eu/

(cc) BY-SA

5.3 External Advisory Board

The EMERALD project established an External Advisory Board (EAB) to provide independent guidance and feedback on research and innovation activities related to cloud cybersecurity certification. As defined in the Description of Action (DoA) [5], the EAB consists of four recognised external experts from academia, industry, and the standardisation sector, covering areas such as cybersecurity standardisation, legal and audit aspects, and operational security implementation. The EAB members are:

- Arthur van der Wees (Arthur's Legal). Lawyer with a technological background and European policy advisor.
- Scott Cadzow (Cadzwo Communication Consulting). AI and Cybersecurity Expert, Chair of TC-SAI, ETSI Fellow 2023 (members with remarkable contributions)
- Tony Rutkowski (CIS), software engineer and cybersecurity expert
- George Sharkov (European Software Institute). Cybersecurity expert, former minister for e-Governance (Bulgaria).

Their complementary expertise has contributed to providing different perspectives on the technical developments and potential applications of the EMERALD framework.

During the first 18 months of the project, two EAB meetings were held, in June 2024 and January 2025, as reported in the Dissemination and Communication Report – v1 [2].

During the second reporting period, **four additional EAB sessions were organised**, continuing the Coffee Break Session format introduced in January 2025. These online meetings were designed to encourage focused discussions on specific aspects of the project, combining technical presentations with opportunities for feedback and exchange with the external experts.

All sessions were moderated by Björn Fanta from Fabasoft and featured a technical deep dive delivered by an EMERALD consortium member on a specific project topic, followed by an interactive discussion with the EAB experts.

The **third EAB meeting was held on 13 May 2025.** In this meeting Stefan Schöberl from SCCH delivered a technical deep dive on *CertGraph* and its role within EMERALD, followed by an interactive discussion with the EAB members. The session provided an opportunity to present this research development and gather external perspectives on its approach and potential applications.

The **fourth EAB meeting, held on 30 September 2025**, featured a technical deep dive delivered by Angela Fessl from Know Center, focusing on the EMERALD User Interface (UI) and User Experience (UX). The session provided an opportunity to present the progress made in the design and development of the interface, discuss usability aspects, and gather feedback from the external experts.

The **fifth EAB meeting, held on 5 March 2026**, adopted a slightly extended format to accommodate two technical presentations, delivered by Juncal Alonso and Nico Haas. The technical discussions covered the European Cluster for Cybersecurity Certification (EC3) and the Common Repository of Metrics, two initiatives supporting collaboration and interoperability in cybersecurity certification. The session provided an opportunity to discuss the progress of these activities, their relevance to the EMERALD objectives, and their potential contribution to the wider cybersecurity certification community.

The **sixth and final EAB meeting was organised in October 2026**, towards the end of the project. Unlike previous sessions, which focused on individual technical developments, this meeting

(cc) BY-SA

presented the EMERALD framework as an integrated solution, providing an overview of its main components, functionalities, and potential applications. Particular attention was given to the exploitation potential of the developed technologies, their long-term sustainability, and opportunities for further adoption beyond the project's duration. The session provided an opportunity to discuss these aspects with the external experts, gathering their perspectives on the future use and exploitation of EMERALD's results.

Overall, the EAB meetings supported the exchange of knowledge between the consortium and external experts throughout the project. The progressive focus of the sessions, from initial project objectives to specific technical developments and final framework integration, allowed the EAB to follow the evolution of EMERALD and provide an external perspective on its research and innovation activities.

DRAFT

CC BY-SA

6 Final Assessment of KPIs

This section presents the final assessments of the Key Performance Indicators (KPIs) for communication, dissemination and networking, as defined in deliverable D6.2 [1]. The analysis considers the results achieved throughout the entire project duration (M1–M36), comparing the final values against the established targets, to show the extent to which the project's communication, dissemination, and networking objectives were achieved. Table 5 presents the symbols used to indicate the final status of each KPI.

Table 5. Explanation symbols for the KPIs

🟢	Criterion has been met or exceeded
🟠	Criterion has not been achieved or could not be assessed due to insufficient data
🔴	Criterion has not yet been achieved

The KPIs are grouped according to communication, dissemination, and networking activities (see Table 6, Table 7, and Table 8, respectively). The columns in each table show the tool used to measure each KPI, a brief description of the indicator, the target value established for the entire project duration, the final value achieved at M36, and the corresponding final status**. By the end of the project, the vast majority of KPIs had successfully achieved or exceeded their respective targets,** demonstrating the overall effectiveness of communication, dissemination, and networking activities.

Table 6. EMERALD KPIs for communication and their final status at M36

Tool	KPI	Objective (M1-M36)	Done (M1-M36)	Status
EMERALD website	Yearly visits	>1,500	6,208 2,960 (May25-Oct26)	🟢
	Duration of visits	More than 2 min. for 40% of users	Average: 50s	🟠
	Monthly downloads: • Posters, flyers • Public reports	30 (posters, flyers/press releases) 50 (public reports)	743 (total number of downloads)	🟢
Social media LinkedIn	Regular posts whenever a relevant milestone is taking place (e.g., event, releases, etc.)	>= 36 posts	128	🟢
Flyers	Number of flyers produced	>= 3 1. CNR 2. FABAR 3. Tecnalia	3	🟢

(cc) BY-SA

Tool	KPI	Objective (M1-M36)	Done (M1-M36)	Status
Press releases	Number of specialized press releases	>= 2 per country in the project, translated into the partners language	2 (consortium) 2 (partners)	
EMERALD fragments	Number of entries	>= 6 per year	79	

Table 7. EMERALD KPIs for dissemination and their final status at M36

Tool	KPI	Objective (M1-M36)	Done (M1-M36)	Status
Journal publications	N. of publications submitted to international scientific journals	>= 2	1	
Conference publications	N. of publications accepted by international scientific conferences	>= 10	13	
EMERALD News (Annual Summary)	N. of annual summaries published	= 1 per year	3	
Posters	N. of posters related to EMERALD	>= 1 per year	4	
Project showcases	N. of demonstration videos produced	>= 6	10	
Participation in events	N. of events attended in which EMERALD (or parts of) is presented or exhibited	>= 5 per year	28	
Cloud Community Publications	N. of references in external sources (e.g., project websites, Collaboration and Support Actions)	> 15	30	

Table 8. EMERALD KPIs for networking and their final status at M36

Tool	KPI	Objective (M1-M36)	Done (M1-M36)	Status
Technological collaborations	Join forces in enhancing and developing	At least one technological asset	2 • Security metrics repository • OSCAL collaboration with COBALT	
Co-organized events	Workshops and/or satellite events and/or joint sessions	>= 2	10 (see Section 5.1)	

(cc) BY-SA

Tool	KPI	Objective (M1-M36)	Done (M1-M36)	Status
Joint dissemination	Joint papers and/or news articles	>= 2	5 • EC3 website • 2 joint publications • 2 joint blogposts	
Working groups	Participation in working groups	>= 3	4 • ETSI • Helen Hub • EUROSCAL • EU Alliance for Industrial Data, Edge and Cloud	

DRAFT

CC BY-SA

7 Conclusions

This deliverable presents the results of the communication, dissemination, and networking activities carried out throughout the 36 months of the EMERALD project, with particular emphasis on the second reporting period (M19–M36). Building on the strategy defined in D6.2 [1] and the activities documented in the previous version of the Dissemination and Communication Report [2], the consortium continued to promote the project's objectives, technical developments, and results, engaging relevant stakeholders and strengthening collaboration within the European cybersecurity community.

Communication activities ensured the continued visibility of EMERALD through a **combination of digital channels and dedicated promotional materials**. The project website remained the main reference point for accessing information and publicly available results, recording **more than 6,000 visits throughout the project**. The regular publication of EMERALD fragments proved particularly effective, with a total of **approximately 80 contributions covering technical developments**, project achievements, events, and other relevant topics. **LinkedIn became the main social media platform** following the discontinuation of activities on X, supporting engagement with professional audiences and the promotion of project-related content. Communication efforts were further complemented by **two flyers and a consortium press release;** the latter translated into the languages of all the participating partners to support wider dissemination.

Scientific dissemination represented another important achievement, with the consortium producing **publications addressing different aspects of cybersecurity certification, automated compliance assessment, security metrics, and evidence management**. During the second reporting period, **nine additional scientific contributions were produced**, bringing the **overall number of publications to fourteen**. EMERALD partners also participated in international conferences, workshops, webinars, and industrial events, presenting research findings and engaging with scientific and industrial communities.

As the project progressed towards its final stages, dissemination activities increasingly focused on **presenting the integrated EMERALD framework** and demonstrating its practical applications. In particular, eight additional videos were produced during the second reporting period, including an overview of the framework, UI/UX mock-ups, and technical demonstrations of the main Compliance-as-a-Service functional streams. Together with the **updated project presentations**, **two additional annual summaries**, and other dissemination materials, these resources contributed to making the project's results more accessible to different audiences and supporting their potential reuse and uptake.

Networking activities also achieved significant results, particularly through **the consolidation and expansion of the European Cluster for Cybersecurity Certification**. Established during the first reporting period, **the cluster evolved into an active collaboration platform involving nine European research projects**. Joint workshops, webinars, conference sessions, and exploitation-oriented initiatives strengthened cooperation and facilitated the exchange of experiences and research findings. Technical collaboration progressed through the **Collaborative Metrics Repository and cooperation on OSCAL**, supporting interoperability and the reuse of security metrics and compliance-related information. Engagement with **standardisation-related initiatives and the External Advisory Board** further contributed to knowledge exchange and provided external perspectives on the project's technical developments and final results.

The final assessment of the communication, dissemination, and networking KPIs confirms that **the activities implemented throughout the project largely achieved their intended objectives**, with several indicators exceeding their initial targets. Overall, the activities carried out within

(cc) BY-SA

WP6 contributed to increasing EMERALD's visibility, disseminating its scientific and technical achievements, and establishing connections with relevant European research and innovation communities. The communication materials, publicly accessible resources, scientific publications, and collaborative initiatives developed throughout the project provide a basis for continued knowledge sharing and support the potential adoption and exploitation of EMERALD's results beyond the project's duration.

DRAFT

CC BY-SA

8 References

[1] EMERALD Consortium, “D6.2 Dissemination and Communication Strategy,” 2024.

[2] EMERALD Consortium, “D6.4 Dissemination and Communication Report - v1,” 2025.

[3] EMERALD Consortium, “D6.7 Exploitation Report - v2,” 2026.

[4] EMERALD Consortium, “D6.1 Project flyer and public website,” 2024.

[5] EMERALD Consortium, “EMERALD - Annex 1 - Description of Action - GA 101120688,” 2022.

DRAFT

CC BY-SA

APPENDIX A Flyers

This section contains the second and the third flyers[40] produced for the project (Figure 30, Figure 31, Figure 32 and Figure 33).

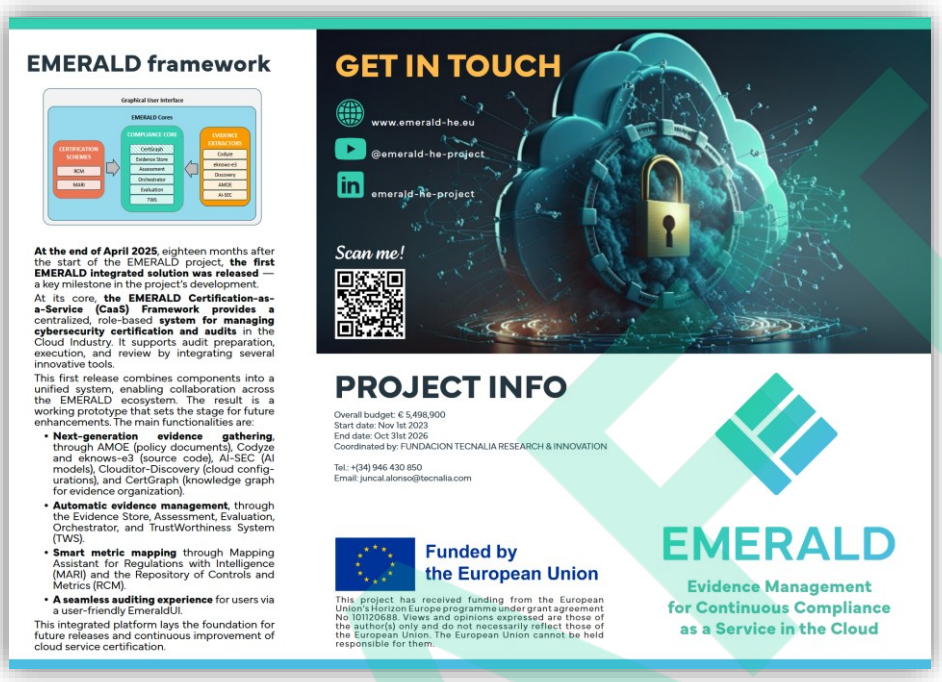


Figure 30. Outer panel of the second EMERALD flyer

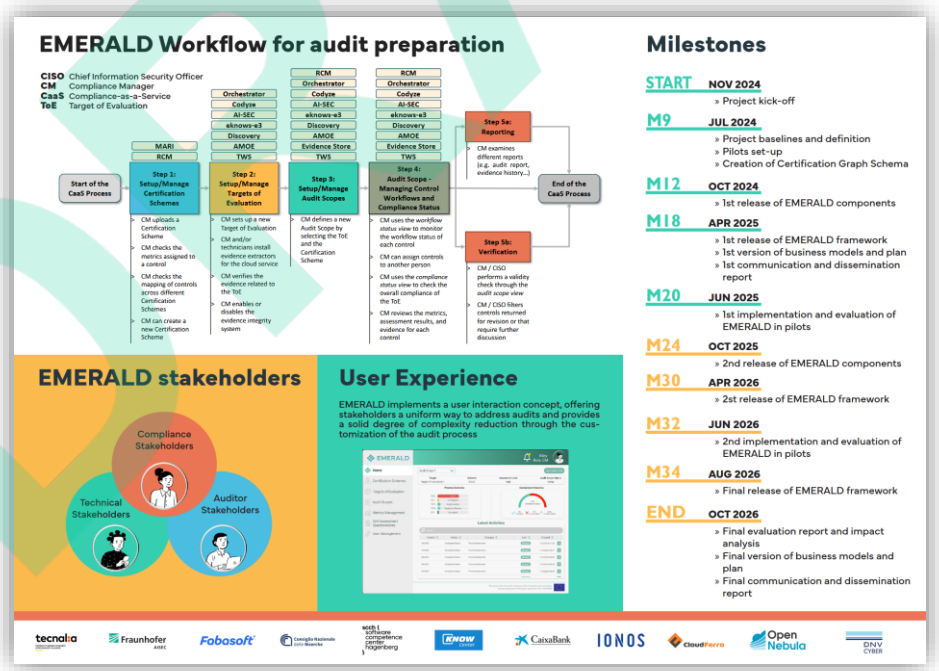


Figure 31. Inner panel of the second EMERALD flyer

[40] https://www.emerald-he.eu/flyers/

(cc) BY-SA



Figure 32. Outer panel of the third EMERALD flyer

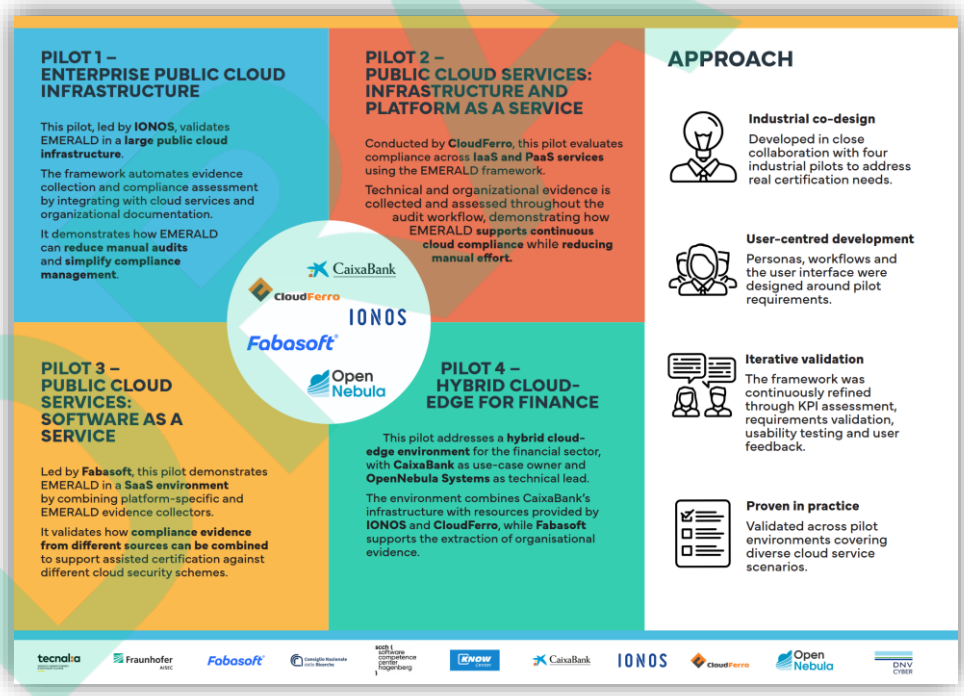


Figure 33. Inner panel of the third EMERALD flyer

CC BY-SA

APPENDIX B Press Release in different languages

The following figures (from Figure 34 to Figure 39) show the content of the second EMERALD press release[41] in English and translated into the different languages of the partners, namely in Finnish, German, Italian, Polish, and Spanish.



EMERALD

Press release

EU-funded project delivers an integrated Compliance-as-a-Service framework validated across four real-world pilots. EMERALD completes its journey towards continuous cloud certification.

Pisa, Italy, October 2026

The EU-funded **EMERALD project (Evidence Management for Continuous Certification as a Service in the Cloud)** has completed its three-year research and innovation programme, **delivering an integrated Compliance-as-a-Service (CaaS) framework** designed to support more continuous, automated and evidence-based approaches to cloud certification.

Bringing together **11 partners from six European countries** (Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula and DNV/Nixu), EMERALD has combined expertise in cloud computing, cybersecurity, artificial intelligence, certification and software engineering to address the growing complexity of compliance in cloud environments. The final framework achieved requirements, across all pilots, bringing together the technical developments produced throughout the project into a common operational environment.

EMERALD demonstrates how innovative technologies can help make cybersecurity compliance more continuous, efficient and evidence based. By bringing together automated evidence collection, assessment and certification in an integrated environment, the project provides a strong foundation for future cloud certification approaches.

From evidence collection to certification

A key achievement of EMERALD is the integration of different sources of certification evidence. The evidence extractors developed in the project (Clouditor-Discovery, Codyze, eknows-e3, AI-SEC and AMOE) **are able to collect and analyse evidence from cloud infrastructures, applications and source code, machine learning models and documents, respectively.**

These different types of evidence are brought together through **CertGraph**, a graph-based knowledge structure that provides a common representation of certification information. CertGraph enables evidence to be linked, combined and traced back to its original source, supporting a more consistent approach to automated assessment.

EMERALD also developed **AIOX**, an AI-assisted tool that helps experts extend the certification ontology when new security metrics are introduced. The tool identifies concepts that are not yet represented and suggests their relationships and placement, while keeping human experts responsible for validating the proposed changes.

The project's assessment and certification components were integrated into a common workflow through the **EMERALD Orchestrator**. This workflow connects evidence management with the **Repository of Controls and Metrics** and intelligent regulatory **Mapping and Assessment functions**, enabling collected evidence to be evaluated against selected security metrics and certification requirements.

The **Trustworthiness System** further supports the integrity and authenticity of evidence and assessment results through blockchain-based verification.

Validation through four pilots

The integrated solution was tested through **four pilots**, covering different cloud service models, organisational contexts and certification needs:

- **Pilot 1, led by IONOS**, evaluated EMERALD in a large public cloud environment, combining infrastructure, source-code, organisational and AI-related evidence and exploring its use for continuous compliance monitoring.
- **Pilot 2, led by CloudFerro**, tested the framework across both Infrastructure-as-a-Service and Platform-as-a-Service environments, combining evidence from OpenStack and Kubernetes with organisational evidence extracted from policy documents.
- **Pilot 3, led by Fabasoft**, explored assisted certification for a cloud-based software environment, including scenarios related to EUCS and BSI C5, and demonstrated the integration of dedicated evidence collectors with the common EMERALD workflow.
- **Pilot 4, led by CaixaBank and OpenNebula**, validated the framework in a hybrid cloud-edge environment for the financial sector, applying requirements based on ENS, ISO 27001, NIST and CIS and testing evidence collection across distributed infrastructures.

The pilot activities combined technical testing with mini-audits, final audits, business-driven evaluation criteria, impact KPIs and user feedback. The results provided evidence of the EMERALD CaaS framework's applicability, identified practical opportunities for improvement and supported the final evaluation of its usability, effectiveness and potential impact.

Supporting Europe's cybersecurity certification ecosystem

Alongside technology development and validation, EMERALD has contributed to wider European collaboration on cybersecurity certification. The project founded and contributed to the European Cluster for Cybersecurity Certification (EC3) bringing together nine European projects working on next-generation certification approaches. EMERALD has also contributed to activities related to **OSCAL and ETSI**, supporting interoperable and machine-readable approaches to security controls, metrics and evidence. The project also participated in the Third Cohort of the European Blockchain Sandbox with one of the components of the EMERALD CaaS Framework, namely the Trustworthiness System.

Project Website

https://www.emerald-he.eu

LinkedIn

https://www.linkedin.com/company/emerald-he-project

Contact:

FUNDACION TECNALIA RESEARCH & INNOVATION

Tel.: +(34) 946 430 850

Email: juncal.alonso@tecnalia.com

Funded by the European Union

This project has received funding from the European Union's Horizon Europe programme under grant agreement No 101120688. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

Figure 34. Second EMERALD press release in English

[41] https://www.emerald-he.eu/press-release/

(cc) BY-SA



EMERALD

Lehdistötiedote

Pisa, Italia, lokakuu 2026

EU-rahoitteinen EMERALD-hanke (Evidence Management for Continuous Certification as a Service in the Cloud) on päättänyt kolmivuotisen tutkimus- ja innovaatio-ohjelmansa. Hankkeen tuloksena syntyi integroitu Compliance-as-a-Service (CaaS) -viitekehys, joka tukee jatkuvaa, automatisoitua ja todisteisiin tukeutuvaa lähestymistapaa pilvipalveluiden sertifiointiin.

EMERALD kokosi yhteen 11 kumppania kuudesta Euroopan maasta: Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula sekä DNV Cyber. Hanke kokosi yhteen pilvipalveluiden, kyberturvallisuuden, tekoälyn, sertifioinnin ja ohjelmistoteknikan asiantuntemuksen vastatakseen pilvimpäristöjen vaatimustenmukaisuuden arvioinnin kasvavaan monimutkaisuuteen. Lopullinen viitekehys täytti kaikissa pilooteissa tunnistetut vaatimukset ja kokosi hankkeen aikana kehitetyt teknologiset ratkaisut yhteiseen toimintaympäristöön.

EMERALD osoittaa, kuinka tietoturvalliset ja innovatiiset teknologiat voivat tehdä kyberturvallisuuden vaatimustenmukaisuudesta jatkuvampaa, tehokkaampaa ja näyttöön perustuvaa. Yhdistämällä automatisoidun todisteiden keruun, arviointiin ja sertifiointiin yhteen ympäristöön hanke luo vahvan perustan tulevaisuuden pilvipalvelusertifioinnille.

Todisteiden keruusta sertifiointiin

Yksi EMERALDin merkittävimmistä saavutuksista on eri sertifiointitodisteiden lähteiden integrointi. Hankkeessa kehitetyt todisteiden keräimet (Clouditor-Discovery, Codyze, eknows-e3, AI-SEC ja AMOE) pystyvät keräämään ja analysoimaan näyttöä vaatimustenmukaisuudesta pilvi-infrastruktuurista, sovelluksista, lähdekoodista, koneoppimismalleista sekä dokumenteista.

Nämä erilaiset lähteet yhdistetään **CertGraphin** avulla. CertGraph on graafipohjainen tietorakenne, joka tarjoaa yhteisen esitysmuodon sertifiointitiedolle. Sen avulla todisteet voidaan linkittää, yhdistää ja jäljittää alkuperäiseen lähteeseensä, mikä tukee yhdenmukaista automaattista arviointia.

EMERALDissa kehitettiin myös **AIOX**, tekoälyavusteinen kehitystyökalu, joka auttaa asiantuntijoita laajentamaan sertifiointi-ontologiaa uusien tietoturvamittareiden käyttöönoton yhteydessä. Työkalu tunnistaa puuttuvia käsitteitä sekä ehdottaa niiden suhteita ja sijoittumista ontologiassa, samalla kun lopullinen validointivastuu säilyy ihmisasiantuntijoilla.

Arviointi- ja sertifiointikomponentit integroitiin yhteiseen työnkulkuun **EMERALD Orchestratorin** avulla. Työnkulku yhdistää todistusaineiston hallinnan, kontrollien ja mittarien tietovaraston sekä älykkäät vaatimustenmukaisuuteen liittyvät kartoitus- ja arviointitoiminnot. Näin kerättyä todistusaineistoa voidaan arvioida valittuja tietoturvamittareita ja sertifiointivaatimuksia vasten.

Trustworthiness System tukee lisäksi todisteiden ja arviointitulosten eheyttä ja aitoutta lohkoketjuteknologian avulla toteutetun varmennuksen kautta.

Validointi neljän pilotin avulla

Integroitua ratkaisua testattiin neljässä pilotissa, jotka kattoivat erilaisia pilvipalvelumalleja, organisaatioympäristöjä ja sertifiointitarpeita:

Pilotti 1 (IONOS): arvioi EMERALDia suuren julkisen pilven ympäristössä yhdistäen infrastruktuuri-, lähdekoodi-, organisaatio- ja tekoälyyn liittyvää todistusaineistoa sekä tutkien jatkuvaa vaatimustenmukaisuuden seurantaa.

Pilotti 2 (CloudFerro): testasi viitekehystä sekä Infrastructure-as-a-Service- että Platform-as-a-Service -ympäristöissä hyödyntäen OpenStackista, Kubernetesista ja organisaatiodokumenteista kerättyä todistusaineistoa.

Pilotti 3 (Fabasoft): tarkasteli avustettua sertifiointia pilvipohjaisessa ohjelmistoympäristössä, mukaan lukien EUCS- ja BSI C5 -skenaariot, sekä toteutti räätälöidyn todisteiden keräinten integroinnin EMERALDin yhteiseen työnkulkuun.

Pilotti 4 (CaixaBank ja OpenNebula): validoi finanssialalle tyypillisen kokoonpanon hybridissä cloud-edge -ympäristössä. Pilotissa sovellettiin ENS-, ISO 27001-, NIST- ja CIS-vaatimuksia sekä testattiin todisteiden keruuta hajautetuissa infrastruktuureissa.

Pilotit yhdistivät teknisen testauksen, miniauditoinnit, loppuauditoinnit, liiketoimintalähtöiset arviointikriteerit, vaikutusmittarit (KPI:t) sekä käyttäjäpalautteen. Tulokset osoittivat EMERALD CaaS -viitekehyksen sovellettavuuden, tunnistivat käytännön kehitysmahdollisuuksia ja tukivat käytettävyyden, tehokkuuden ja vaikutusten lopullista arviointia.

Euroopan kyberturvallisuuden sertifiointiekosysteemin tukeminen

Teknologian kehittämisen ja validoinnin lisäksi EMERALD on osallistunut laajempaan eurooppalaiseen yhteistyöhön kyberturvallisuuden sertifioinnin alueella. Hanke perusti ja tuki European Cluster for Cybersecurity Certification (EC3) -verkostoa, joka kokoaa yhteen yhdeksän eurooppalaista hanketta kehittämään seuraavan sukupolven sertifiointimenetelmiä. Lisäksi EMERALD osallistui OSCAL- ja ETSI-työhön edistäen yhteentoimivia ja koneellisesti luettavia lähestymistapoja tietoturvakontrolleihin, mittareihin ja todistusaineistoon. Hanke osallistui myös European Blockchain Sandboxin kolmanteen kohorttiin Trustworthiness System -komponentillaan.

Projektin kotisivu
https://www.emerald-he.eu
LinkedIn
https://www.linkedin.com/company/emerald-he-project
Tiedustelut:
FUNDACION TECNALIA RESEARCH & INNOVATION
Tel.: +(34) 946 430 850

Email: juncal.alonso@tecnalia.com

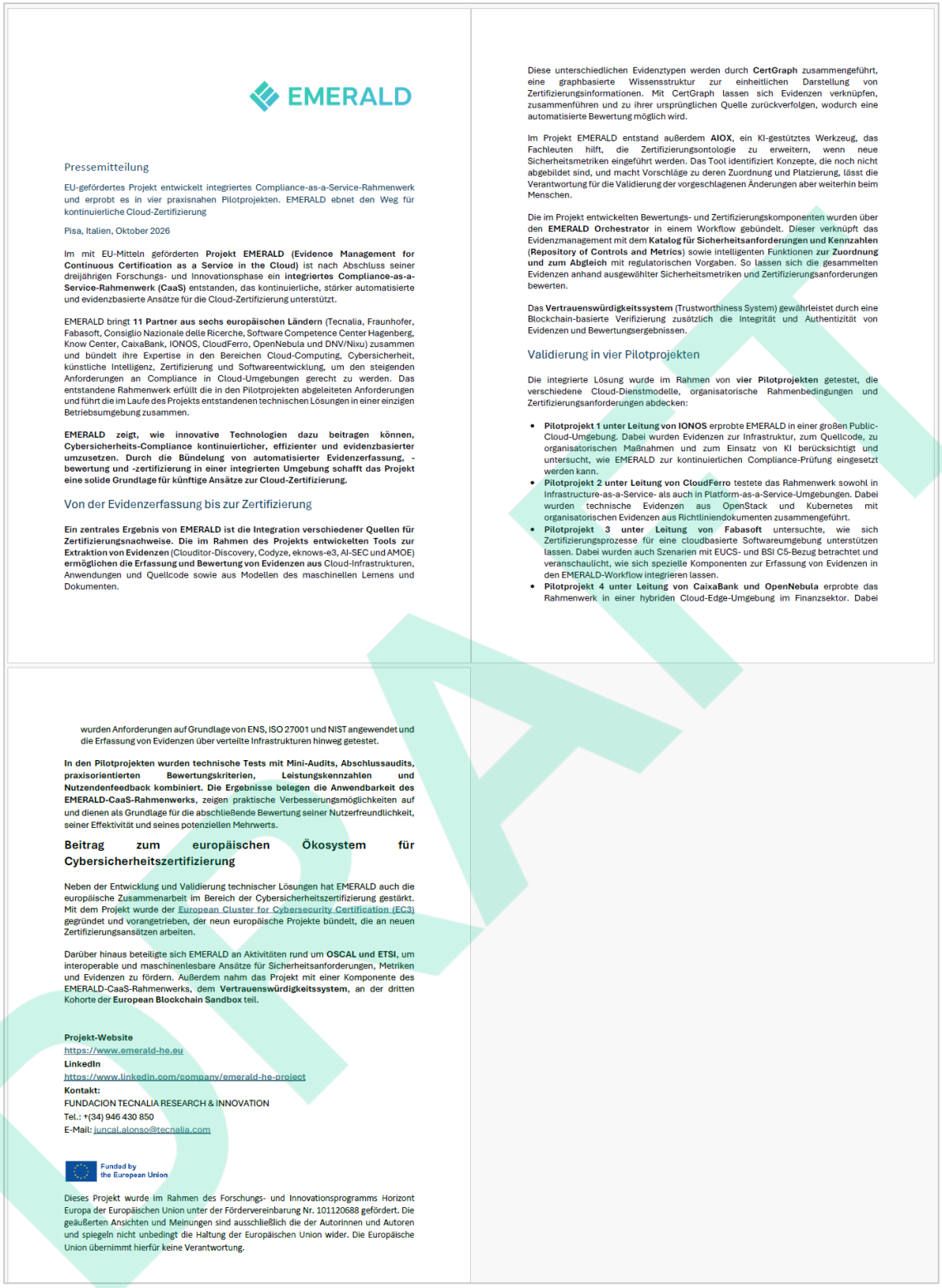
Funded by the European Union

Tämä hanke on saanut rahoitusta Euroopan unionin Horizon Europe -ohjelmasta avustussopimuksen nro 101120688 nojalla. Esitetyt näkemykset ja mielipiteet ovat ainoastaan kirjoittajan/kirjoittajien omia, eivätkä välttämättä vastaa Euroopan unionin näkemyksiä. Euroopan unioni ei ole niistä vastuussa.

Figure 35. Second EMERALD Press Release translated into Finnish

DRAFT

CC BY-SA



EMERALD

Pressemitteilung

EU-gefördertes Projekt entwickelt integriertes Compliance-as-a-Service-Rahmenwerk und erprobt es in vier praxisnahen Pilotprojekten. EMERALD ebnet den Weg für kontinuierliche Cloud-Zertifizierung

Pisa, Italien, Oktober 2026

Im mit EU-Mitteln geförderten **Projekt EMERALD (Evidence Management for Continuous Certification as a Service in the Cloud)** ist nach Abschluss seiner dreijährigen Forschungs- und Innovationsphase ein **integriertes Compliance-as-a-Service-Rahmenwerk (CaaS)** entstanden, das kontinuierliche, stärker automatisierte und evidenzbasierte Ansätze für die Cloud-Zertifizierung unterstützt.

EMERALD bringt **11 Partner aus sechs europäischen Ländern** (Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula und DNV/Nixu) zusammen und bündelt ihre Expertise in den Bereichen Cloud-Computing, Cybersicherheit, künstliche Intelligenz, Zertifizierung und Softwareentwicklung, um den steigenden Anforderungen an Compliance in Cloud-Umgebungen gerecht zu werden. Das entstandene Rahmenwerk erfüllt die in den Pilotprojekten abgeleiteten Anforderungen und führt die im Laufe des Projekts entstandenen technischen Lösungen in einer einzigen Betriebsumgebung zusammen.

EMERALD zeigt, wie innovative Technologien dazu beitragen können, Cybersicherheits-Compliance kontinuierlicher, effizienter und evidenzbasierter umzusetzen. Durch die Bündelung von automatisierter Evidenzerfassung, -bewertung und -zertifizierung in einer integrierten Umgebung schafft das Projekt eine solide Grundlage für künftige Ansätze zur Cloud-Zertifizierung.

Von der Evidenzerfassung bis zur Zertifizierung

Ein zentrales Ergebnis von EMERALD ist die Integration verschiedener Quellen für Zertifizierungsnachweise. Die im Rahmen des Projekts entwickelten Tools zur Extraktion von Evidenzen (Clouditor-Discovery, Codyze, eknows-e3, AI-SEC und AMOE) **ermöglichen die Erfassung und Bewertung von Evidenzen aus** Cloud-Infrastrukturen, Anwendungen und Quellcode sowie aus Modellen des maschinellen Lernens und Dokumenten.

Diese unterschiedlichen Evidenztypen werden durch **CertGraph** zusammengeführt, eine graphbasierte Wissensstruktur zur einheitlichen Darstellung von Zertifizierungsinformationen. Mit CertGraph lassen sich Evidenzen verknüpfen, zusammenführen und zu ihrer ursprünglichen Quelle zurückverfolgen, wodurch eine automatisierte Bewertung möglich wird.

Im Projekt EMERALD entstand außerdem **AIOX**, ein KI-gestütztes Werkzeug, das Fachleuten hilft, die Zertifizierungsontologie zu erweitern, wenn neue Sicherheitsmetriken eingeführt werden. Das Tool identifiziert Konzepte, die noch nicht abgebildet sind, und macht Vorschläge zu deren Zuordnung und Platzierung, lässt die Verantwortung für die Validierung der vorgeschlagenen Änderungen aber weiterhin beim Menschen.

Die im Projekt entwickelten Bewertungs- und Zertifizierungskomponenten wurden über den **EMERALD Orchestrator** in einem Workflow gebündelt. Dieser verknüpft das Evidenzmanagement mit dem **Katalog für Sicherheitsanforderungen und Kennzahlen (Repository of Controls and Metrics)** sowie intelligenten Funktionen **zur Zuordnung und zum Abgleich** mit regulatorischen Vorgaben. So lassen sich die gesammelten Evidenzen anhand ausgewählter Sicherheitsmetriken und Zertifizierungsanforderungen bewerten.

Das **Vertrauenswürdigkeitssystem** (Trustworthiness System) gewährleistet durch eine Blockchain-basierte Verifizierung zusätzlich die Integrität und Authentizität von Evidenzen und Bewertungsergebnissen.

Validierung in vier Pilotprojekten

Die integrierte Lösung wurde im Rahmen von **vier Pilotprojekten** getestet, die verschiedene Cloud-Dienstmodelle, organisatorische Rahmenbedingungen und Zertifizierungsanforderungen abdecken:

- **Pilotprojekt 1 unter Leitung von IONOS** erprobte EMERALD in einer großen Public-Cloud-Umgebung. Dabei wurden Evidenzen zur Infrastruktur, zum Quellcode, zu organisatorischen Maßnahmen und zum Einsatz von KI berücksichtigt und untersucht, wie EMERALD zur kontinuierlichen Compliance-Prüfung eingesetzt werden kann.
- **Pilotprojekt 2 unter Leitung von CloudFerro** testete das Rahmenwerk sowohl in Infrastructure-as-a-Service- als auch in Platform-as-a-Service-Umgebungen. Dabei wurden technische Evidenzen aus OpenStack und Kubernetes mit organisatorischen Evidenzen aus Richtliniendokumenten zusammengeführt.
- **Pilotprojekt 3 unter Leitung von Fabasoft** untersuchte, wie sich Zertifizierungsprozesse für eine cloudbasierte Softwareumgebung unterstützen lassen. Dabei wurden auch Szenarien mit EUCS- und BSI C5-Bezug betrachtet und veranschaulicht, wie sich spezielle Komponenten zur Erfassung von Evidenzen in den EMERALD-Workflow integrieren lassen.
- **Pilotprojekt 4 unter Leitung von CaixaBank und OpenNebula** erprobte das Rahmenwerk in einer hybriden Cloud-Edge-Umgebung im Finanzsektor. Dabei

wurden Anforderungen auf Grundlage von ENS, ISO 27001 und NIST angewendet und die Erfassung von Evidenzen über verteilte Infrastrukturen hinweg getestet.

In den Pilotprojekten wurden technische Tests mit Mini-Audits, Abschlussaudits, praxisorientierten Bewertungskriterien, Leistungskennzahlen und Nutzendenfeedback kombiniert. Die Ergebnisse belegen die Anwendbarkeit des EMERALD-CaaS-Rahmenwerks, zeigen praktische Verbesserungsmöglichkeiten auf und dienen als Grundlage für die abschließende Bewertung seiner Nutzerfreundlichkeit, seiner Effektivität und seines potenziellen Mehrwerts.

Beitrag zum europäischen Ökosystem für Cybersicherheitszertifizierung

Neben der Entwicklung und Validierung technischer Lösungen hat EMERALD auch die europäische Zusammenarbeit im Bereich der Cybersicherheitszertifizierung gestärkt. Mit dem Projekt wurde der European Cluster for Cybersecurity Certification (ECS) gegründet und vorangetrieben, der neun europäische Projekte bündelt, die an neuen Zertifizierungsansätzen arbeiten.

Darüber hinaus beteiligte sich EMERALD an Aktivitäten rund um **OSCAL und ETSI**, um interoperable und maschinenlesbare Ansätze für Sicherheitsanforderungen, Metriken und Evidenzen zu fördern. Außerdem nahm das Projekt mit einer Komponente des EMERALD-CaaS-Rahmenwerks, dem **Vertrauenswürdigkeitssystem**, an der dritten Kohorte der **European Blockchain Sandbox** teil.

Projekt-Website
https://www.emerald-he.eu
LinkedIn
https://www.linkedin.com/company/emerald-he-project
Kontakt:
FUNDACION TECNALIA RESEARCH & INNOVATION
Tel.: +(34) 946 430 850
E-Mail: juncal.alonso@tecnalia.com

Funded by the European Union

Dieses Projekt wurde im Rahmen des Forschungs- und Innovationsprogramms Horizont Europa der Europäischen Union unter der Fördervereinbarung Nr. 101120688 gefördert. Die geäußerten Ansichten und Meinungen sind ausschließlich die der Autorinnen und Autoren und spiegeln nicht unbedingt die Haltung der Europäischen Union wider. Die Europäische Union übernimmt hierfür keine Verantwortung.

Figure 36. Second EMERALD Press Release translated into German

(cc) BY-SA



EMERALD

Nota stampa

Il progetto EMERALD, finanziato dall'UE, conclude il percorso verso la certificazione continua dei servizi cloud e realizza un framework integrato di Compliance-as-a-Service validato in quattro progetti pilota in contesti reali

Pisa, Ottobre 2026

Il **progetto europeo EMERALD (Evidence Management for Continuous Certification as a Service in the Cloud)** ha completato il suo programma triennale di ricerca e innovazione, **realizzando un framework integrato di Compliance-as-a-Service (CaaS)** progettato per rendere la certificazione dei servizi cloud più continua, automatizzata e basata su evidenze.

Con **11 partner provenienti da sei Paesi europei** (Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula e DNV/Nixu) EMERALD ha riunito competenze in cloud computing, cybersicurezza, intelligenza artificiale, certificazione e ingegneria del software per affrontare la crescente complessità della conformità in ambienti cloud. Il framework finale ha soddisfatto i requisiti di tutti i progetti pilota, integrando in un ambiente operativo comune le soluzioni tecnologiche sviluppate nel corso del progetto. EMERALD **dimostra come le tecnologie innovative possano rendere la verifica della conformità ai requisiti di cybersicurezza più continua, efficiente e basata su evidenze. Integrando in un unico ambiente la raccolta automatizzata delle evidenze, la valutazione e la certificazione, il progetto pone solide basi per futuri approcci alla certificazione di servizi cloud.**

Dalla raccolta delle evidenze alla certificazione

Un risultato chiave di EMERALD è l'integrazione di diverse fonti di evidenza e supporto della certificazione. Gli strumenti di estrazione sviluppati nell'ambito del progetto — Clouditor-Discovery, Codyze, eknows-e3, AI-SEC e AMOE — consentono, rispettivamente, di raccogliere e analizzare evidenze provenienti da infrastrutture cloud, applicazioni e codice sorgente, modelli di machine learning e documenti.

Queste diverse tipologie di evidenze confluiscono in **CertGraph**, una struttura di conoscenza basata su grafi che fornisce una rappresentazione comune delle informazioni necessarie alla certificazione. CertGraph permette di collegare e combinare le evidenze e di risalire alla loro fonte originale, favorendo una maggiore coerenza nella valutazione automatizzata.

EMERALD ha inoltre sviluppato **AIOX**, uno strumento basato sull'intelligenza artificiale che aiuta gli esperti a estendere l'ontologia di certificazione quando si introducono nuove metriche di sicurezza. Lo strumento identifica concetti non ancora rappresentati e ne suggerisce le relazioni e la collocazione nell'ontologia, lasciando agli esperti umani la responsabilità di validare le modifiche proposte.

I componenti di valutazione e certificazione del progetto sono stati integrati in un flusso di lavoro comune attraverso l'**EMERALD Orchestrator**. Tale flusso collega la gestione delle evidenze al **Repository of Controls and Metrics** e alle funzionalità intelligenti di **MARI**, lo strumento intelligente che mappa requisiti normativi e metriche di sicurezza. Questo abilita la valutazione delle evidenze raccolte rispetto sia alle metriche di sicurezza che ai requisiti di certificazione selezionati.

Il **Trustworthiness System** garantisce inoltre l'integrità e l'autenticità delle evidenze e dei risultati delle valutazioni attraverso meccanismi di verifica basati su blockchain.

La validazione attraverso quattro progetti pilota

La soluzione integrata è stata testata attraverso quattro progetti pilota, che hanno interessato diversi modelli di servizi cloud, contesti organizzativi ed esigenze di certificazione:

- **Il primo progetto pilota, guidato da IONOS**, ha valutato EMERALD in un ambiente di cloud pubblico su larga scala, combinando evidenze relative all'infrastruttura, al codice sorgente, ad aspetti organizzativi e all'intelligenza artificiale, esplorandone l'utilizzo per il monitoraggio continuo della conformità.
- **Il secondo progetto pilota, guidato da CloudFerro,** ha sperimentato il framework in ambienti Infrastructure-as-a-Service e Platform-as-a-Service, combinando evidenze provenienti da OpenStack e Kubernetes con evidenze organizzative estratte da documenti di policy.
- **Il terzo progetto pilota, guidato da Fabasoft**, ha esplorato la certificazione assistita di un ambiente software basato sul cloud, includendo scenari relativi a EUCS e BSI C5, e ha dimostrato l'integrazione di strumenti specifici per la raccolta delle evidenze nel flusso di lavoro comune di EMERALD.
- **Il quarto progetto pilota, guidato da CaixaBank e OpenNebula**, ha validato il framework in un ambiente ibrido cloud-edge per il settore finanziario, applicando requisiti basati su ENS, ISO 27001, NIST e CIS e testando la raccolta delle evidenze su infrastrutture distribuite.

Le attività dei progetti pilota hanno combinato test tecnici con mini-audit, audit finali, criteri di valutazione legati alle esigenze aziendali, indicatori chiave di prestazione (KPI) per la misura dell'impatto e feedback degli utenti. I risultati hanno fornito riscontri sull'applicabilità del framework Caas di EMERALD, individuato opportunità concrete di miglioramento e contribuito alla valutazione finale della sua usabilità, efficacia e potenziale impatto.

A sostegno dell'ecosistema europeo della certificazione di cybersicurezza

Parallelamente allo sviluppo e alla validazione tecnologica, EMERALD ha contribuito ad una più ampia collaborazione europea in materia di certificazione di cybersicurezza. Il progetto ha contribuito alla nascita e alle attività dello European Cluster for Cybersecurity Certification (EC3) che riunisce nove progetti europei impegnati nello sviluppo di approcci di certificazione di nuova generazione. EMERALD ha inoltre contribuito ad attività relative a **OSCAL** ed **ETSI**, sostenendo approcci interoperabili e leggibili dalle macchine per la rappresentazione di requisiti di sicurezza, metriche ed evidenze. Il progetto ha anche partecipato al terzo gruppo di progetti selezionati per lo European Blockchain Sandbox con il Trustworthiness System, uno dei componenti del framework CaaS di EMERALD.

Sito Web del Progetto
https://www.emerald-he.eu

LinkedIn
https://www.linkedin.com/company/emerald-he-project

Contatti:
FUNDACION TECNALIA RESEARCH & INNOVATION
Tel.: +(34) 946 430 850
Email: juncal.alonso@tecnalia.com

Funded by the European Union

Il progetto ha ricevuto finanziamenti dal programma Horizon Europe dell'Unione europea nell'ambito dell'accordo di sovvenzione n. 101120688. Le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione europea. L'Unione europea non può esserne ritenuta responsabile.

DRAFT

Figure 37. Second EMERALD Press Release translated into Italian

CC BY-SA



EMERALD

Nota de prensa

Un proyecto financiado por la UE ofrece un marco integrado de "Compliance-as-a-Service" validado en cuatro proyectos piloto en condiciones reales. EMERALD culmina su trayectoria hacia la certificación continua en la nube

Bilbao, octubre 2026

El **proyecto EMERALD (Evidence Management for Continuous Certification as a Service in the Cloud)** ha completado su programa de investigación e innovación de tres años, **ofreciendo un marco integrado de "Compliance-as-a-Service" (CaaS)** diseñado para apoyar enfoques más continuos, automatizados y basados en evidencias para la certificación en la nube.

La reunión de **11 socios de seis países europeos** (Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula y DNV/Nixu), ha permitido a EMERALD combinar experiencia en computación en la nube, ciberseguridad, inteligencia artificial, certificación e ingeniería de software para poder abordar la creciente complejidad del cumplimiento normativo en entornos cloud. El marco final de EMERALD cumple con los requisitos identificados en todos los pilotos, integrando los avances técnicos logrados a lo largo del proyecto en un entorno operativo común.

EMERALD demuestra cómo las tecnologías innovadoras pueden contribuir a que el cumplimiento de las normas de ciberseguridad sea más continuo, eficiente y basado en evidencias. Al combinar la recopilación automatizada de pruebas, la evaluación y la certificación en un entorno integrado, el proyecto proporciona una base sólida para futuros enfoques de certificación en la nube.

De la recogida de evidencias a la certificación

Uno de los logros clave de EMERALD es la integración de diferentes fuentes de evidencias de certificación. Los extractores de evidencias desarrollados en el proyecto (Clouditor-Discovery, Codyze, eknows-e3, AI-SEC y AMOE) **son capaces de recopilar y analizar evidencias** procedentes de infraestructuras cloud, aplicaciones y código fuente, modelos de aprendizaje automático y documentos, respectivamente.

Estos diferentes tipos de evidencia se agrupan a través de **CertGraph**, una estructura de conocimiento basada en grafos que proporciona una representación común de la información de certificación. CertGraph permite vincular, combinar y rastrear las evidencias hasta su fuente original, lo que favorece un enfoque más coherente en una evaluación automatizada.

EMERALD también ha desarrollado **AIOX**, una herramienta asistida por IA que ayuda a los expertos a ampliar la ontología de certificación cuando se introducen nuevas métricas de seguridad. La herramienta identifica conceptos que aún no están representados y sugiere sus relaciones y ubicación, al tiempo que deja en manos de los expertos humanos la responsabilidad de validar los cambios propuestos.

Los componentes de evaluación y certificación del proyecto se han integrado en un flujo de trabajo común a través de **EMERALD Orchestrator**. Este flujo de trabajo conecta la gestión de evidencias con el **Repositorio de Controles y Métricas**, así como con funciones inteligentes de **mapeo y evaluación normativo**, permitiendo que la evidencia recopilada sea evaluada en función de las métricas de seguridad y los requisitos de certificación seleccionados.

El **Trustworthiness System** refuerza aún más la integridad y la autenticidad de evidencias y resultados de la evaluación mediante una verificación basada en blockchain.

Validación mediante cuatro proyectos piloto

La solución integrada se ha probado a través de **cuatro proyectos piloto**, que abarcan diferentes modelos de servicio en la nube, contextos organizativos y necesidades de certificación:

- **Piloto 1, liderado por IONOS,** ha evaluado EMERALD en un entorno de nube pública a gran escala, combinando evidencias de infraestructura, código fuente, organizativas y relacionadas con la IA, y explorando su uso para la supervisión continua del cumplimiento normativo.
- **Piloto 2, liderado por CloudFerro,** ha probado el marco tanto en entornos de "infraestructura como servicio" (IaaS) como de "plataforma como servicio" (PaaS), combinando evidencias procedentes de OpenStack y Kubernetes con evidencias organizativas extraídas de documentos normativos.
- **Piloto 3, liderado por Fabasoft**, ha explorado la certificación asistida para un entorno de software basado en la nube, incluyendo escenarios relacionados con EUCS y BSI C5, y ha demostrado la integración de otros colectores de evidencias con los flujos de trabajo de EMERALD.
- **Piloto 4, liderado por CaixaBank y OpenNebula,** ha validado el marco en un entorno híbrido cloud-edge para el sector financiero, aplicando requisitos basados en ENS, ISO 27001, NIST y CIS y probando la recogida de evidencias en infraestructuras distribuidas.

Las actividades de los proyectos piloto han combinado pruebas técnicas con mini-auditorías, auditorías finales, criterios de evaluación orientados al negocio, KPIs de impacto y comentarios de los usuarios. Los **resultados han demostrado la aplicabilidad del marco CaaS de EMERALD**, identificado oportunidades prácticas de mejora y servido de base para la evaluación final de su usabilidad, eficacia e impacto potencial.

Apoyando el ecosistema europeo de certificación de ciberseguridad

Además del desarrollo y la validación de la tecnología, EMERALD ha contribuido a una mayor colaboración europea en materia de certificación de ciberseguridad. El proyecto ha fundado y colaborado con el Clúster Europeo para la Certificación en Ciberseguridad (EC3), que agrupa a nueve proyectos europeos dedicados al desarrollo de enfoques de certificación de última generación. EMERALD también ha contribuido a actividades relacionadas con **OSCAL** y **ETSI**, apoyando enfoques interoperables y legibles por máquina para controles de seguridad, métricas y evidencias. El proyecto también ha participado en la tercera edición del **European Blockchain Sandbox** con uno de los componentes del marco CaaS de EMERALD, concretamente el Trustworthiness System.

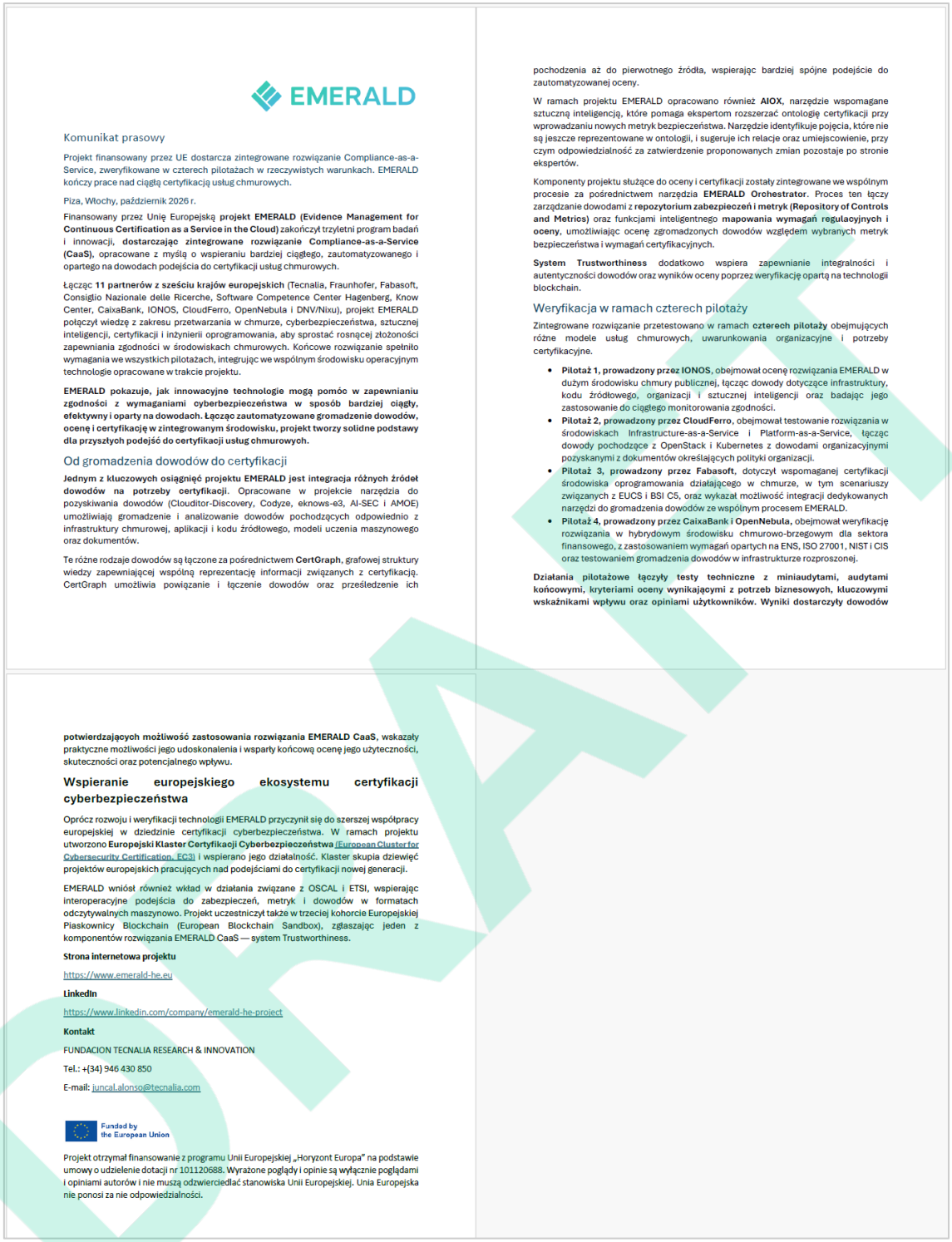
Sitio web del proyecto:
https://www.emerald-he.eu
LinkedIn:
https://www.linkedin.com/company/emerald-he-project
Contacto:
FUNDACION TECNALIA RESEARCH & INNOVATION
Tel.: +(34) 946 430 850
Email: juncal.alonso@tecnalia.com

Funded by the European Union

This project has received funding from the European Union's Horizon Europe programme under grant agreement No 101120688. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

Figure 38. EMERALD Press Release translated into Spanish

CC BY-SA



EMERALD

Komunikat prasowy

Projekt finansowany przez UE dostarcza zintegrowane rozwiązanie Compliance-as-a-Service, zweryfikowane w czterech pilotażach w rzeczywistych warunkach. EMERALD kończy prace nad ciągłą certyfikacją usług chmurowych.

Piza, Włochy, październik 2026 r.

Finansowany przez Unię Europejską **projekt EMERALD (Evidence Management for Continuous Certification as a Service in the Cloud)** zakończył trzyletni program badań i innowacji, **dostarczając zintegrowane rozwiązanie Compliance-as-a-Service (CaaS)**, opracowane z myślą o wspieraniu bardziej ciągłego, zautomatyzowanego i opartego na dowodach podejścia do certyfikacji usług chmurowych.

Łącząc **11 partnerów z sześciu krajów europejskich** (Tecnalia, Fraunhofer, Fabasoft, Consiglio Nazionale delle Ricerche, Software Competence Center Hagenberg, Know Center, CaixaBank, IONOS, CloudFerro, OpenNebula i DNV/Nixu), projekt EMERALD połączył wiedzę z zakresu przetwarzania w chmurze, cyberbezpieczeństwa, sztucznej inteligencji, certyfikacji i inżynierii oprogramowania, aby sprostać rosnącej złożoności zapewniania zgodności w środowiskach chmurowych. Końcowe rozwiązanie spełniło wymagania we wszystkich pilotażach, integrując we wspólnym środowisku operacyjnym technologie opracowane w trakcie projektu.

EMERALD pokazuje, jak innowacyjne technologie mogą pomóc w zapewnianiu zgodności z wymaganiami cyberbezpieczeństwa w sposób bardziej ciągły, efektywny i oparty na dowodach. Łącząc zautomatyzowane gromadzenie dowodów, ocenę i certyfikację w zintegrowanym środowisku, projekt tworzy solidne podstawy dla przyszłych podejść do certyfikacji usług chmurowych.

Od gromadzenia dowodów do certyfikacji

Jednym z kluczowych osiągnięć projektu EMERALD jest integracja różnych źródeł dowodów na potrzeby certyfikacji. Opracowane w projekcie narzędzia do pozyskiwania dowodów (Clouditor-Discovery, Codyze, eknows-e3, AI-SEC i AMOE) umożliwiają gromadzenie i analizowanie dowodów pochodzących odpowiednio z infrastruktury chmurowej, aplikacji i kodu źródłowego, modeli uczenia maszynowego oraz dokumentów.

Te różne rodzaje dowodów są łączone za pośrednictwem **CertGraph**, grafowej struktury wiedzy zapewniającej wspólną reprezentację informacji związanych z certyfikacją. CertGraph umożliwia powiązanie i łączenie dowodów oraz prześledzenie ich pochodzenia aż do pierwotnego źródła, wspierając bardziej spójne podejście do zautomatyzowanej oceny.

W ramach projektu EMERALD opracowano również **AIOX**, narzędzie wspomagane sztuczną inteligencją, które pomaga ekspertom rozszerzać ontologię certyfikacji przy wprowadzaniu nowych metryk bezpieczeństwa. Narzędzie identyfikuje pojęcia, które nie są jeszcze reprezentowane w ontologii, i sugeruje ich relacje oraz umiejscowienie, przy czym odpowiedzialność za zatwierdzenie proponowanych zmian pozostaje po stronie ekspertów.

Komponenty projektu służące do oceny i certyfikacji zostały zintegrowane we wspólnym procesie za pośrednictwem narzędzia **EMERALD Orchestrator**. Proces ten łączy zarządzanie dowodami z **repozytorium zabezpieczeń i metryk (Repository of Controls and Metrics)** oraz funkcjami inteligentnego **mapowania wymagań regulacyjnych i oceny**, umożliwiając ocenę zgromadzonych dowodów względem wybranych metryk bezpieczeństwa i wymagań certyfikacyjnych.

System Trustworthiness dodatkowo wspiera zapewnianie integralności i autentyczności dowodów oraz wyników oceny poprzez weryfikację opartą na technologii blockchain.

Weryfikacja w ramach czterech pilotaży

Zintegrowane rozwiązanie przetestowano w ramach **czterech pilotaży** obejmujących różne modele usług chmurowych, uwarunkowania organizacyjne i potrzeby certyfikacyjne.

- **Pilotaż 1, prowadzony przez IONOS**, obejmował ocenę rozwiązania EMERALD w dużym środowisku chmury publicznej, łącząc dowody dotyczące infrastruktury, kodu źródłowego, organizacji i sztucznej inteligencji oraz badając jego zastosowanie do ciągłego monitorowania zgodności.
- **Pilotaż 2, prowadzony przez CloudFerro**, obejmował testowanie rozwiązania w środowiskach Infrastructure-as-a-Service i Platform-as-a-Service, łącząc dowody pochodzące z OpenStack i Kubernetes z dowodami organizacyjnymi pozyskanymi z dokumentów określających polityki organizacji.
- **Pilotaż 3, prowadzony przez Fabasoft**, dotyczył wspomaganej certyfikacji środowiska oprogramowania działającego w chmurze, w tym scenariuszy związanych z EUCS i BSI C5, oraz wykazał możliwość integracji dedykowanych narzędzi do gromadzenia dowodów ze wspólnym procesem EMERALD.
- **Pilotaż 4, prowadzony przez CaixaBank i OpenNebula,** obejmował weryfikację rozwiązania w hybrydowym środowisku chmurowo-brzegowym dla sektora finansowego, z zastosowaniem wymagań opartych na ENS, ISO 27001, NIST i CIS oraz testowaniem gromadzenia dowodów w infrastrukturze rozproszonej.

Działania pilotażowe łączyły testy techniczne z miniaudytami, audytami końcowymi, kryteriami oceny wynikającymi z potrzeb biznesowych, kluczowymi wskaźnikami wpływu oraz opiniami użytkowników. Wyniki dostarczyły dowodów potwierdzających możliwość zastosowania rozwiązania EMERALD CaaS, wskazały praktyczne możliwości jego udoskonalenia i wsparły końcową ocenę jego użyteczności, skuteczności oraz potencjalnego wpływu.

Wspieranie europejskiego ekosystemu certyfikacji cyberbezpieczeństwa

Oprócz rozwoju i weryfikacji technologii EMERALD przyczynił się do szerszej współpracy europejskiej w dziedzinie certyfikacji cyberbezpieczeństwa. W ramach projektu utworzono **Europejski Klaster Certyfikacji Cyberbezpieczeństwa** (European Cluster for Cybersecurity Certification, EC3) i wspierano jego działalność. Klaster skupia dziewięć projektów europejskich pracujących nad podejściami do certyfikacji nowej generacji.

EMERALD wniósł również wkład w działania związane z OSCAL i ETSI, wspierając interoperacyjne podejścia do zabezpieczeń, metryk i dowodów w formatach odczytywalnych maszynowo. Projekt uczestniczył także w trzeciej kohorcie Europejskiej Piaskownicy Blockchain (European Blockchain Sandbox), zgłaszając jeden z komponentów rozwiązania EMERALD CaaS — system Trustworthiness.

Strona internetowa projektu

https://www.emerald-he.eu

LinkedIn

https://www.linkedin.com/company/emerald-he-project

Kontakt

FUNDACION TECNALIA RESEARCH & INNOVATION

Tel.: +(34) 946 430 850

E-mail: juncal.alonso@tecnalia.com

Funded by the European Union

Projekt otrzymał finansowanie z programu Unii Europejskiej „Horyzont Europa" na podstawie umowy o udzielenie dotacji nr 101120688. Wyrażone poglądy i opinie są wyłącznie poglądami i opiniami autorów i nie muszą odzwierciedlać stanowiska Unii Europejskiej. Unia Europejska nie ponosi za nie odpowiedzialności.

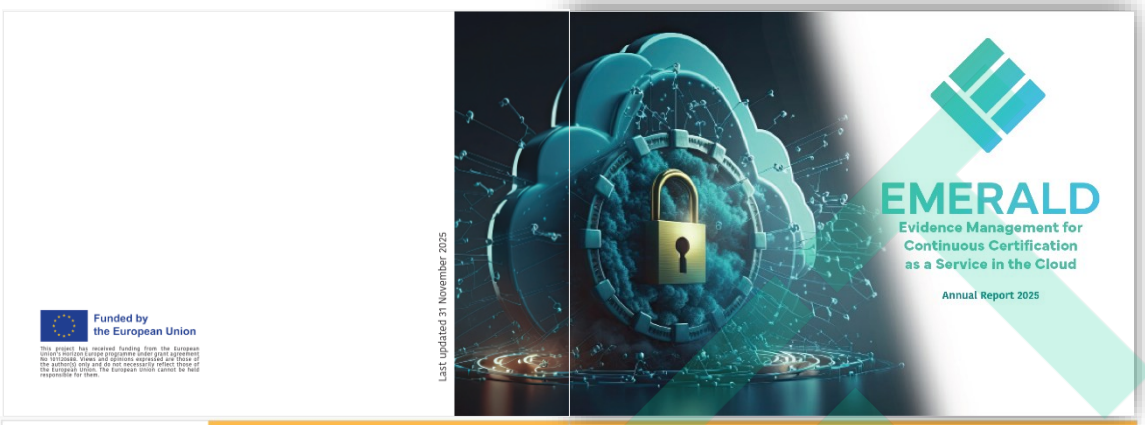
Figure 39. Second EMERALD Press Release translated into Polish

CC BY-SA

APPENDIX C EMERALD News

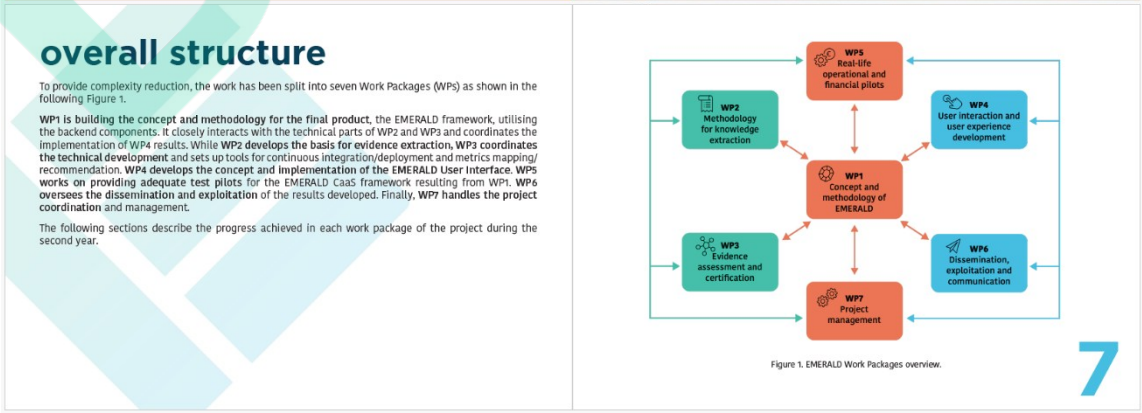
This appendix reports the content of the second and the third EMERALD annual summaries[42].

Second EMERALD annual summary









[42] https://www.emerald-he.eu/annual-summaries/

(cc) BY-SA

WP1
FRAMEWORK DESIGN AND METHODOLOGICAL BLUEPRINT

WP1 is responsible for defining and implementing the **architecture of the EMERALD CaaS framework**, as well as the **DevOps strategy and the integration** of its components. During the second year, significant progress was made: data modelling was refined, components were fully defined, and interaction mechanisms (APIs) were completed. The integration environment was also deployed, and the DevOps methodology was implemented, ensuring smooth and rapid collaboration between developers and enabling the automatic deployment of the EMERALD framework.

The second version of the EMERALD components was released and made available in the EMERALD public repository at the end of October 2025 (https://git.code.tecnalia.dev/emerald/public), with 82% of the technical requirements already fulfilled. Consequently, the **first prototype of the EMERALD Compliance-as-a-Service (CaaS) framework** was deployed, integrating nearly all components on the Kubernetes (k8s) platform (Figure 2).

The technical stack supporting this work includes **OpenStack** as the infrastructure provider, **Ansible** for Infrastructure as Code (IaC), **Docker** for containerization, **Artifactory** as the image registry, **GitLab** agents in the pipelines, **Semantic Releases** for versioning, **Kubernetes** as the deployment platform, **Keycloak** as the identity manager, **Longhorn** for storage, **Nginx** as proxy, and **Rancher** as a web-based monitoring and debugging interface.

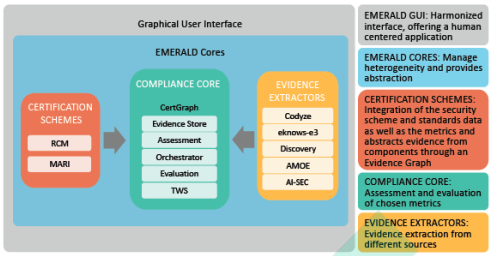


Figure 2. EMERALD components overview.

WP2
ADVANCED TECHNIQUES FOR EVIDENCE AND INSIGHT EXTRACTION

The main goal of WP2 is **to establish a unified view** of the **target of evaluation** – the cloud service or system undergoing certification – by extracting, interpreting, and combining **evidence from multiple layers**, including infrastructure, software, and AI layers (Figure 3). Over the past 12 months, WP2 has made significant progress in refining the knowledge extraction methodology and supporting tools.

- AMOE, the component for organizational evidence gathering, was enhanced to provide more flexible and efficient extraction of security-related information from documentation. It is now better integrated into the EMERALD user interface and workflows, with improvements that make evidence handling more structured and reliable.
- AI-SEC component continued to mature as a toolkit for evaluating the security of Artificial Intelligence models, with improvements in usability and functionality. Over the last year, it has been significantly extended to extract and evaluate security-relevant evidence directly from ML models, extending EMERALD with new model-level assurance capabilities.
- Clouditor-Discovery, now renamed simply Discovery, collects evidence about the secure configuration of cloud resources. During the last year, it was extended to cover additional cloud environments and services, increasing the range of infrastructure and platform-level evidence that can be collected. Furthermore, its integration into the EMERALD ecosystem was further consolidated.
- Codyze, used to identify critical security-related functionalities, was refined to better fit within the common EMERALD workflow, focusing on more effective and centralized extraction and handling of security evidence. Its integration with other project components was strengthened, improving consistency and interoperability.
- The eknows-e3 evidence extractor was further developed and stabilized during the last year, with improved integration into development workflows and broader support for extracting security-relevant information from source code. Its overall coverage and maturity have increased, making it more suitable for systematic evidence collection.

Finally, a new AI-assisted ontology refinement tool now supports the integration of security concepts into the certification graph.

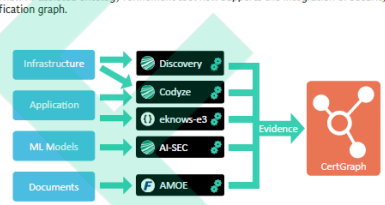


Figure 3. Evidence extraction tools of EMERALD.

WP3
AUTOMATED ASSESSMENT AND CERTIFICATION FRAMEWORK

The main objective of WP3 is to enable continuous certification decisions based on a target of evaluation constantly changing over time, thus it serves as **an integration point for the evidence collection and knowledge extraction tools of WP2**. The work carried out during the last year has enabled the integration of the components (metrics, ontology, repository, orchestrator, TWS, etc.) into a single, coordinated framework. Below, an overview of the progress for each task is reported.

- **Graph-based Representation of Cloud Service Evidence.** This task **integrates into the Orchestrator the certification graph concept as defined in WP2**, which provides the current state of the certification graph. The graph database work advances toward **ontology-aligned, multi-layer evidence**. A hybrid format metric format was adopted: **human- and machine-readable,** to support both **governance and review** as well as **automated reasoning and cross-system interoperability**. To foster broader collaboration with other EU projects, we created a new **common Security Metrics Repository** (https://github.com/Cybersecurity-Certification-Hub/security-metrics) to share and expand the set of available metrics.
- **Repository of Controls and Metrics.** This task produces **a smart catalogue of Controls and Metrics** for EMERALD. In the last period, the schema was extended for greater flexibility and multi-scheme support **beyond EUCS**, aligning with EMERALD's data model and ontology. **BSICS and AIC4 were integrated** into the catalogue, and **OSCAL templates** for EUCS import/export, C5, and AIC4 were defined. The tool can already export data to Excel or OSCAL formats and import from OSCAL, while importing from Excel is still in progress. **The metric data model was refined** to accommodate a larger set of metrics, and **mappings across different certification schemes were enhanced**.
- **Metric Selection and Optimization for Cloud Certifications.** This task provides an intelligent system that can **select an optimal set of metrics to be associated with one -or more- certification scheme(s)**. The Mapping Assistant for Regulation with Intelligence (MARI) tool, based on a deep learning sentence transformer architecture, improved significantly during the last year. The tool can currently perform both control-to-control and metric-to-control mappings across different certification schemes.
- **Evaluation and Assessment of Metrics based on the Knowledge Graph.** Based on the metrics selected by the MARI and the integration performed in the Orchestrator, this task **combines (pre-existing) assessment and evaluation tools** into the EMERALD framework. **The Common Metrics Repository now includes over 70 metrics**, with new ones generated through scripts and templates, assisted by AI tools. The final compliance decision module was implemented within the Orchestrator, enabling automatic pass/fail decisions based on the aggregated evaluation results. On the assessment side, the TrustWorthiness System (TWS) integration has begun, to ensure the integrity of assessment results. For the Evidence Store, lightweight database solutions were evaluated, with in-memory testing completed and a production-ready database selected for deployment.
- **Blockchain-based Trust System for Auditors.** This task focuses the TWS, which **leverages blockchain technologies to ensure evidence integrity during its whole lifecycle**. The TWS has been deployed on **the Alastria network** and is being integrated with the EMERALD interface, including secure handling of evidence and assessment results. In parallel, regulatory and policy aspects relevant to the TWS have been addressed through **participation in the third European Blockchain Sandbox cohort**.

WP4
USER-CENTERED INTERFACE DESIGN AND IMPLEMENTATION

The overall goal of WP4 is to develop **an integrated EMERALD User Interface** that is tailored to the users' needs during all stages of an audit. To achieve this goal, WP4 is proceeding along four streams in line with the four tasks of WP4.

Requirements engineering with compliance managers and auditors. During the second project year, we have conducted a set of interviews and focus groups with our target groups (e.g., auditors, compliance managers) from the different pilot partners, to understand their working tasks in relation to preparing and conducting audits. As a result, **we have elicited a set of 25 requirements** for the UI/UX development.

Modelling work processes. For developing the work processes, we have developed a set **of seven personas** who represent the target users of EMERALD that were already presented in the first year. For each persona, we have developed a Persona-on-the-go (Figure 4) representing **a concise visual summary** highlighting key characteristics of each user type. Additionally, we have developed 14 different scenarios, which serve as the basis for understanding **user journeys and interactions**.

Furthermore, through our co-creation and co-design approach – consisting of interviews, focus groups, and workshops – we were able to derive ten simple processes and ten elaborated workflow representations. Based on these, we developed a **universally applicable blueprint for implementing EMERALD in audit** preparation and audit execution workflows, which may be valuable for other companies seeking to use the EMERALD solution to enhance their audit preparation processes or to support audit executions.



Figure 4. Example of "persona-on-the-go" for the Compliance Manager Riley.

Designing a user interaction and user experience concept. With the insights gained from the previous activities, we have developed a **full set of clickable mock-ups using a co-creation and co-design process**, where we iteratively discussed and improved them together with the pilot partners and component owners.

Implementation of EMERALD UI. The implementation of the EMERALD UI is **based on the mock-ups and workflow processes** described above. It is based on NextJS and React and designed as a modular container, that integrates seamlessly into the EMERALD framework architecture and CI/CD processes. Authentication is handled by the EMERALD central Keycloak service, which issues user tokens for accessing EMERALD components API. Currently, the RCM, AMOE and Orchestrator components are integrated, while additional components – such as the EvidenceStore and TWS – are being tested. **Additional API endpoints and EMERALD functionalities** will be introduced over the coming months, along with continuous user and pilot testing.

CC BY-SA

WP5
PILOTS DEPLOYMENTS AND FRAMEWORK VALIDATION STRATEGY

The goal of WP5 is to demonstrate how the EMERALD solution can **manage and monitor the certification of cloud services** according to the needs of the different pilot scenarios. To achieve this, the business-driven requirements for the pilots (BDRP), Key Performance Indicators (KPIs) and goals for the pilots were **periodically aligned with the EMERALD components**. The pilots are part of two categories, with Category 1 focusing on the certification of public cloud services (Pilot 1-3), and Category 2 focusing on the certification of hybrid cloud-edge environments for the financial sector (Pilot 4). Figure 5 depicts one of the pilot/EMERALD workflows, illustrating the different roles and communication flows within the project.

WP5 developed a validation plan to generate iterative feedback for the technical work packages. The validation plan includes a so-called **stage-gate process, designed to verify the validity of the developed tools and to enable structured feedback to the EMERALD components**. With the insights gained at each stage-gate, the project can be adjusted to the needs of the different stakeholders.

Discussions and demo sessions with the technical project partners have allowed the pilots to derive a **personalized, yet scalable scenario for continuous cloud certification processes**. Data exchange and refinement of the evidence extraction tools are an ongoing process.

The pilots as well as the component owners are working on the **implementation of metrics to address different controls and security requirements** from security schemes such as the EUCS and BSI-C5.

These metrics will facilitate the evidence extraction by the EMERALD components and allow for the integration of pilot-specific audit goals. In order to fulfil this, the EMERALD and pilot-specific evidence extraction tools are deployed and tested. The testing phase has now been extended to include the EMERALD UI.

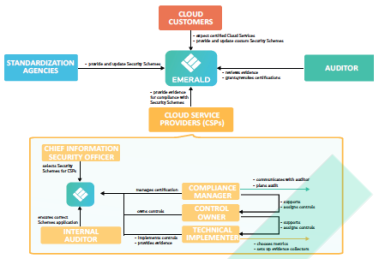


Figure 5. EMERALD pilots' workflow.

WP6
IMPACT OPTIMIZATION THROUGH TARGETED STAKEHOLDER COLLABORATION

WP6 focuses on **maximizing the visibility and impact of the EMERALD project**, ensuring that its results are effectively disseminated, communicated, exploited, and aligned with standardization activities. During the second year of the project, significant progress was achieved across all tasks.

Dissemination and communication efforts during the last year included the design, development, and publication of the **second EMERALD flyer**, updates to the project website, and the creation of a dedicated **Zenodo community** (https://zenodo.org/communities/emerald-he-project) for sharing project outputs. The monthly "Emerald Fragments" continued to be published, with several contributions shared according to the social media/fragments rotation schedule across multiple content categories. Additionally, EMERALD was **presented to academic and industrial audiences** through seminars and conferences.

Networking activities strengthened collaboration through the creation of the **European Cluster for Cybersecurity Certification (EC3)** (https://cybersecuritycertcluster.eu/), a forum designed to bring together research and innovation initiatives addressing Next Generation Agile Certification (Figure 6). The cluster aims to foster collaboration among EU-funded projects, enabling them to share experiences, align approaches, and discuss challenges for adoption and future research. Regular **meetings with the External Advisory Board** (EAB) were held to gather feedback on EMERALD's progress and to review ongoing developments.

Exploitation activities concentrated on **consolidating EMERALD's value propositions** and **business models**. Early exploitation plans were further developed through workshops and preparatory meetings with partner projects, aiming to align strategies with technical progress and stakeholder needs.

Standardization activities **advanced EMERALD's alignment with recognized frameworks and regulatory developments**. The project progressed in integrating OSCAL standards into its components, participated in relevant forums, engaged with ETSI, and developed a **Common Metrics Repository**.



Figure 6. Website of the European Cluster for Cybersecurity Certification.

WP7
EFFICIENT MANAGEMENT AND DELIVERABLE TRACKING

WP7 focuses on providing structured project management to **ensure EMERALD progresses smoothly, adhering to timeline, budget, and quality standards**. Through WP7, the consortium has established robust coordination mechanisms and reporting tools, fostering effective collaboration across all partners and WPs.

In its second year, WP7 made effective use of the **essential project structures**, including regular follow-up meetings, document-sharing on the Fabasoft Cloud, and efficient digital communication tools. TECNALIA, which is leading this WP, organized two **General Assemblies** in Pisa and Linz, and several **monthly teleconferences to monitor progress and coordinate activities**, addressing emerging issues and promoting transparency. A key milestone was the compilation and submission of the Project Management Report for the first reporting period, which documents the technical and outreach progress achieved in the first 18 months of the project, as well as an analysis of deviations and risks.

To maintain quality, WP7 followed the templates and review protocols set up in the **Project Manual and Quality Plan** to guarantee the quality of all project deliverables. A total of 20 deliverables have been successfully submitted, several of which also passed through a security review performed by the Security Advisory Board.

The Risk Register was updated during the second Interim technical report and the Periodic report, thus **facilitating early issue detection and timely intervention**. The **Innovation Management Plan** has been implemented, ensuring the soundness and innovation of the EMERALD outcomes in collaboration with the Project Manager, the Technical Manager, the Exploitation and Innovation Manager, and the technical WPs leaders. Input has been received from the External Advisory Board, whose members have provided external oversight to ensure that EMERALD's innovations align with industry and technical standards.

Data management and privacy are also priorities in WP7, with a GDPR-compliant Data Management Plan, setting **standards for data collection, storage, and ethical handling**, both in project tasks and in the interviews conducted in the Pilots to support the design of the EMERALD UI/UX.

Moving forward, WP7 will sustain its oversight of timely deliverables, continue **fostering collaboration across partners,** and **reinforce** the **engagement with the Security Advisory Board and the External Advisory Board** for additional expert guidance and validation. Project management will remain responsible for **monitoring resource allocation** in line with the plan, identifying and addressing instances of overspending and underspending, and ensuring that partners meet their commitments and that the outcomes established in the Description of Action (DoA) are successfully achieved.

what's next

During the last year, EMERALD has made **substantial progress toward delivering a fully integrated Compliance-as-a-Service (CaaS) solution.**

The project has successfully advanced the architecture, DevOps processes, and integration of technical components, developed a user-centered interface, and validated solutions through diverse pilot scenarios. Dissemination and exploitation activities have strengthened EMERALD's visibility, standardization alignment, and potential for industrial uptake, while structured project management has ensured timely progress, quality, and stakeholder engagement.

Looking ahead, in the final year, EMERALD will focus on **final integration, validation, and refinement** of all components and workflows. This includes completing the deployment of remaining modules, expanding API endpoints, enhancing evidence extraction and metric optimization, and incorporating feedback from pilots to further improve usability and functionality. Efforts will also concentrate on ensuring full alignment with certification schemes, completing standardization activities, and finalizing exploitation and sustainability plans to enable industry adoption. With a focus on quality, security, and user experience, EMERALD is poised to deliver a **scalable, user-friendly, and fully operational CaaS platform** by the end of the project.



(cc) BY-SA

Third EMERALD annual summary



Funded by the European Union

Last updated 30 October 2026

EMERALD

Evidence Management for Continuous Certification as a Service in the Cloud

Annual Report 2026

www.emerald-he.eu
emerald-he-project
@emerald-he-project

contents

Introduction 4
WP1 Final Framework and Integrated EMERALD Solution 8
WP2 Evidence and Knowledge Extraction Results 10
WP3 Automated Assessment and Certification Results 12
WP4 User-Centred Interface: Final Implementation 14
WP5 Pilot Validation and Impact 16
WP6 Dissemination, Exploitation and Strategic Collaboration 18
WP7 Efficient Management and Coordination 20
Beyond EMERALD 22

Introduction:
From Integration to Validation

Building on the foundations established during its first two years, EMERALD has entered its final phase, **turning the Compliance-as-a-Service (CaaS) concept into an integrated and operational solution for continuous cloud certification**. By combining automated evidence collection, intelligent metric mapping, assessment mechanisms and a user-centred interface, the **project supports more efficient, scalable and trustworthy certification processes** across complex cloud environments.

During the third year, the consortium, formed by eleven partners from six countries, **completed the final version of the EMERALD CaaS framework**. The technical components developed across the project were integrated into a common environment, **with all technical requirements fully implemented**. Evidence extraction, certification graph, assessment and orchestration capabilities were consolidated, while the framework was deployed in dedicated environments supporting all four EMERALD pilots.

Pilot validation became a central focus of the project. Three pilots assessed EMERALD in public cloud service scenarios, while the fourth addressed a hybrid cloud-edge environment in the financial sector. Through staged validation, mini-audits, KPI assessment, business-driven requirements verification and user feedback, **the pilots tested the framework under real operational conditions and provided targeted input for its final refinement**.

In parallel, **EMERALD increased the visibility of its results, advanced their exploitation, and strengthened their contribution to standardisation activities**, while maintaining effective coordination and quality assurance across the consortium. As the project approaches completion, attention is shifting from technical development to demonstrated impact, sustainability and future uptake, marking EMERALD's transition from an integrated research outcome to a mature foundation for continuous, evidence-based cloud certification.

overall results

EMERALD's seven Work Packages have contributed to create **complementary results towards a common objective. WP1 coordinated the architecture and integration** of the final Compliance-as-a-Service framework, bringing together the **evidence extraction capabilities developed in WP2**, the **assessment and certification mechanisms created in WP3**, and the **user-centred interface designed in WP4. WP5 connected these technical developments with real certification needs**, using feedback from the four pilots to support their validation and final refinement.

WP6 promoted the dissemination, exploitation and standardisation of the project results through public software and deliverables, scientific publications, showcases, collaboration activities with other EU initiatives and a Common Repository for Security Metrics. Throughout the project, **WP7 supported effective coordination, quality assurance and timely delivery** across the consortium.

The following sections present the main results achieved by each Work Package, **with particular emphasis on pilot validation and the overall impact of the EMERALD solution**.

7

CC BY-SA

WP1
FINAL FRAMEWORK AND INTEGRATED EMERALD SOLUTION

WP1 is responsible for the **architecture, integration and continuous deployment of the EMERALD CaaS framework** (Figure 1). Building on the first integrated prototype presented in the previous year, work during the final project phase focused on consolidating component interactions, completing the remaining technical requirements and preparing a stable solution for pilot validation.

The **second release of the integrated framework was completed in April 2026**, incorporating updated versions of the technical components and extending their integration within the environment. This was followed in August 2026 by the **third and final release of the EMERALD CaaS framework**, which brought together the developments completed across the technical Work Packages and incorporated the refinements introduced during the last project months. The publicly available EMERALD components can be accessed through the project's public GitLab repository.

The final release **consolidated component interactions, APIs and data flows across the framework**. The implementation of the technical requirements was brought close to completion, while interoperability and deployment procedures were further verified.

The supporting infrastructure was expanded from three to seven Kubernetes nodes and now provides **one integration environment and four dedicated pilot environments**. Automated CI/CD pipelines continued to support the building, deployment and verification of new component versions, ensuring consistency between the integration and pilot environments.

As a result, WP1 delivered the **final integrated EMERALD CaaS framework** and provided the technical foundation required for its validation across the four pilots.

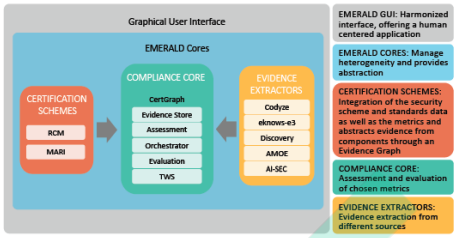


Figure 1. EMERALD components overview

WP2
EVIDENCE AND KNOWLEDGE EXTRACTION RESULTS

WP2 aims to provide a **unified view of the target of evaluation** by extracting, structuring and combining certification evidence from different layers of a cloud service. Cloud itor-Discovery collects evidence from cloud infrastructures, Codyze and eknows-e3 analyse source code, AI-SEC evaluates security-relevant properties of machine learning models, and the AMOE tool extracts organisational evidence from policy documents. Together, these tools provide the heterogeneous evidence required by the EMERALD assessment process. By June 2026, the project's evidence extractors had been completed and consolidated.

During the final project year, WP2 also focused on the **refinement and completion of the CertGraph ontology**. CertGraph provides a common graph-based structure in which evidence produced by the different extractors can be semantically linked, combined and traced back to its original source. This enables evidence from different layers to be retrieved and interpreted as part of a unified representation of the target of evaluation.

The final ontology consists of a common core covering evidence, framework elements, functionalities, properties and security concepts, **complemented by domain-specific extensions for cloud infrastructure, applications, machine learning models, documents and human resources** (Figure 2). The cloud, machine learning and document extensions were refined based on the security metrics developed in EMERALD, while a new Human Resources (HR) extension was introduced in response to pilot requirements, to model organisational evidence related to personnel, including roles, responsibilities, qualifications, training and involvement in security-relevant processes.. This modular structure supports the consistent evolution and future extension of the CertGraph.

WP2 also developed **AIOX, an AI-assisted Ontology Extension Tool**, to help experts extend *CertGraph* **when new security metrics are introduced**. AIOX analyses metric specifications, identifies concepts not yet represented in the ontology, and suggests their placement and relationships. These recommendations remain subject to human validation, **ensuring that experts retain control over changes to the ontology** (Figure 2).

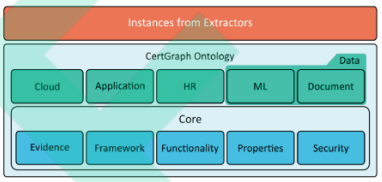


Figure 2. Updated design of the CertGraph ontology.

WP3
AUTOMATED ASSESSMENT AND CERTIFICATION RESULTS

WP3 provides the **assessment and certification capabilities at the core of the EMERALD CaaS framework**. Its components transform the evidence collected by WP2 into evaluation results and certification decisions, supporting continuous assessment across different cybersecurity schemes. During the final project year, the work focused on **completing the integration of the WP3 components into a coordinated certification workflow.**

The **Orchestrator now connects the Evidence Store, Assessment and Evaluation components with the Repository of Controls and Metrics (RCM) and the Mapping Assistant for Regulation with Intelligence (MARI)**. Through this workflow, evidence represented according to CertGraph can be assessed against selected metrics, aggregated at control level and used to support automated compliance decisions. **The integration of the RCM with MARI and AMOE was completed**, together with its **connection to the common Security Metrics Repository**[1], facilitating the reuse of metrics and mappings across certification schemes.

The **Trustworthiness System was further integrated into this workflow** to protect the integrity and authenticity of evidence and assessment results through blockchain-based verification. **An automatic verification service was introduced** to compare information stored within EMERALD against the proofs of integrity recorded on the blockchain. A dedicated viewer also makes verification results accessible to non-technical users, while integration with the EMERALD User Interface continued to be tested during the final phase.

As a result, WP3 moved from the implementation of individual tools to an **integrated evidence assessment and certification workflow ready for pilot validation**. The final integration supports graph-based evidence management, intelligent metric selection, multi-scheme certification decisions and trustworthy exchange of assessment information, while pilot feedback guided the last technical refinements.

1. https://github.com/Cybersecurity-Certification-Hub/security-metrics

WP4
USER-CENTRED INTERFACE: FINAL IMPLEMENTATION

During the last year of the project, WP4 has transformed the user requirements, personas, workflows and interactive mock-ups, produced during **the earlier project phases, into an integrated EMERALD User Interface** (Figure 3). The interface provides an abstraction layer over the technical components, allowing users to access the main Compliance-as-a-Service functionalities through **coordinated workflows** without interacting directly with the underlying tools.

The final interface is **structured around three complementary visualization streams**.

- **The Certification Schemes stream** enables users to upload, compare and customise certification schemes, manage their controls and use AI-assisted mapping functionalities.
- **The Targets of Evaluation stream** supports the definition of systems undergoing certification, the connection of evidence extraction tools and the management of user access rights.
- Finally, **the Audit Scopes stream** brings schemes and targets together, allowing users to review compliance results, assign responsibilities and support the generation of assessments and reports.

During the final project year, implementation focused on completing these workflows and **extending the connection between the interface and the EMERALD backend**. The UI now integrates core components including the Repository of Controls and Metrics, AMOE, Evidence Store, Orchestrator and Trustworthiness System through their respective APIs. Authentication and role-based access are managed centrally through Keycloak, supporting secure access to functions and information according to each user's responsibilities.

Most of the planned UI functionalities were successfully implemented, turning the design concepts from the initial mock-ups into **an operational interface for audit preparation and execution**. Validation across the four pilots assessed its usability and verified the workflows in realistic settings, **while user feedback guided the final refinements of the interface**.

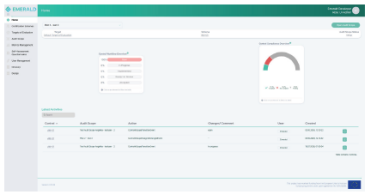


Figure 3. EMERALD User Interface.

(cc) BY-SA

WP5
PILOT VALIDATION AND IMPACT

During the final project year, WP5 moved from pilot preparation to the **operational validation of the integrated EMERALD framework**. The four pilots tested the solution across different cloud service models, organisational contexts and certification needs, providing the main environment for assessing whether the project's technical results could support realistic compliance and audit workflows.

Validation followed **the stage-gate approach defined at the beginning of the project**. Pilot readiness, component deployment and workflow integration were progressively reviewed through preparatory activities, mini-audits and final audits. The process combined technical testing with the assessment of business-driven requirements, pilot-specific and impact KPIs, and user feedback. Results were communicated to the technical Work Packages throughout the process, enabling the final refinement of components, metrics and user workflows.

Pilot 1, led by IONOS, evaluated how EMERALD could be **integrated into the existing systems of a large public cloud provider** and support compliance managers in continuous monitoring. The pilot focused on controls derived from BSI C5 and combined organisational, infrastructure, source-code and AI-related evidence. Discovery was connected to the IONOS Cloud API, while Codyze and eknows-e3 accessed selected software repositories. AMOE supported the analysis of policy documents, and an isolated AI-SEC scenario was established using representative test data. The pilot validated the deployment of these tools and their contribution to a coordinated evidence and assessment workflow.

Pilot 2, led by CloudFerro, tested EMERALD **across both Infrastructure-as-a-Service and Platform-as-a-Service environments**. Two separate OpenStack projects were configured to represent virtual infrastructure and a Kubernetes-based platform. Discovery successfully identified and collected information about deployed cloud resources, while AMOE analysed anonymised organisational policies against selected metrics. The final validation brought these technical and organisational evidence sources together within the EMERALD workflow and assessed their use through the project interface.

Pilot 3, led by Fabasoft, explored assisted certification for a cloud-based software environment, with reference to schemes such as EUCS and BSI C5. In addition to AMOE, the pilot introduced two dedicated tools: the Fabasoft Cloud Evidence Collector, which retrieves information about cloud objects and operational processes, and the App.Telemetry Evidence Collector, which transforms monitoring data into evidence compatible with EMERALD. Their integration demonstrated how pilot-specific collectors can complement the common EMERALD components and contribute evidence to the same certification workflow.

Pilot 4 addressed a hybrid cloud-edge environment for the financial sector, with CaixaBank as use-case owner and OpenNebula Systems as technical lead. An OpenNebula Front-End operated as an Evidence Collection Gateway, coordinating resources across CaixaBank, IONOS and CloudFerro environments. The pilot applied a custom compliance framework based on ENS, ISO 27001, NIST and CIS requirements. Evidence collection through the OpenNebula integration was validated end to end, while AMOE supported organisational evidence from policy documents. The audit activities assessed how EMERALD could support compliance monitoring across distributed infrastructures subject to demanding financial-sector requirements.

Overall, the pilots demonstrated the application of EMERALD to **public cloud, platform, software and hybrid cloud-edge scenarios** and validated the interoperability of evidence extractors, certification schemes, metrics, assessment components and the user interface under realistic conditions. The **results provided evidence of the framework's applicability**.

17

WP6
DISSEMINATION, EXPLOITATION AND STRATEGIC COLLABORATION

During the final project year, WP6 focused on **maximising the visibility, uptake and long-term value of EMERALD's results**. Communication and dissemination activities accompanied the project's transition from technical development to validation, making its final outcomes accessible through the website[2], social media, scientific publications, public deliverables, the Zenodo community[3], project showcases and updated dissemination materials.

Networking activities were strengthened through the European Cluster for Cybersecurity Certification[4] (EC3), which **expanded to nine European projects** working on next-generation cybersecurity certification. The cluster provided a common platform for technical exchange, dissemination and exploitation, supporting joint events on cloud, IoT and supply-chain security, cybersecurity regulation and the future of certification. These activities included collaborative publications, workshops, webinars, roundtables and panels, as well as cross-project exploitation workshops and participation in the ETSI Security Conference 2026. EC3 also supported the sharing of resources and the development of the common Security Metrics Repository.

Exploitation activities were completed for all **nine EMERALD components and for the integrated CaaS framework**. Business

2. https://www.emerald-he.eu/
3. https://zenodo.org/communities/emerald-he-project
4. https://cybersecuritycertcluster.eu/

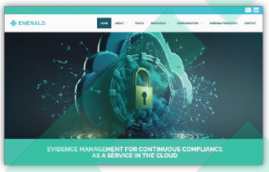


Figure 4. Landing page of the EMERALD project website.

models, value propositions, licensing approaches and target markets were analysed and refined through three exploitation workshops held in Barcelona, Linz and Warsaw. The final strategy considers both the **independent exploitation of components by their respective partners and the potential joint uptake of the integrated EMERALD platform**. An updated analysis of the compliance automation and cloud security market helped position the project's results in relation to commercial and open-source alternatives.

Standardisation work continued through **contributions related to OSCAL, the Common Security Metrics Repository and ETSI**, supporting interoperable and machine-readable approaches to security controls, metrics and evidence. These activities also considered developments connected with EUCS and European regulatory frameworks including the Cyber Resilience Act, NIS2 and DORA. Together, dissemination, exploitation, networking and standardisation strengthened EMERALD's **foundations for continued use and development beyond the project**.

19

WP7
EFFICIENT MANAGEMENT AND COORDINATION

During the final project year, WP7 ensured the **effective coordination and successful completion of EMERALD**, supporting collaboration across the consortium and monitoring the implementation of activities across all Work Packages. Regular follow-up meetings and shared digital tools continued to facilitate communication, decision-making and the timely resolution of emerging issues.

Four General Assemblies were organized in **Linz, Munich, Warsaw and Bilbao**. These meetings provided opportunities to review the project's progress and achievements, coordinate the remaining activities and align the consortium on project closure and future sustainability.

Quality assurance procedures established through the Project Manual and Quality Plan continued to support the preparation, internal review and approval of project outputs. By the end of EMERALD, **49 deliverables had been completed**, documenting the project's methodological, technical, validation, dissemination and management results.

The External Advisory Board continued to provide **independent feedback on selected aspects of the project**. Dedicated sessions allowed consortium partners to present specific developments and receive recommendations on their clarity, relevance and potential areas for improvement. This feedback supported the refinement of project results and helped ensure their alignment with external stakeholder expectations.

WP7 also **updated the Data Management Plan** to reflect the project's final data, software and research outputs. Data management continued to follow GDPR requirements and the project's established principles for secure collection, storage, access and preservation.

Through these activities, WP7 maintained **effective cooperation among the eleven partners and supported the orderly completion** of EMERALD's technical, administrative and reporting commitments.



21

Beyond EMERALD:
Sustainability and Future Uptake

As EMERALD reaches completion, attention is shifting from the development and validation of its results to their **continued use, evolution and adoption beyond the project**. The final Compliance-as-a-Service framework provides a foundation for more automated, evidence-based and user-centred cloud certification, while the pilot activities have demonstrated its applicability across public cloud, software and hybrid cloud-edge environments.

A three-phase sustainability roadmap has been outlined to explore how the project's results could be maintained and further developed. The partners will pursue the exploitation of individual components according to their respective strategies, while also exploring opportunities for the joint uptake of the integrated EMERALD framework. Experience and feedback collected through the four pilots will support future technical improvements, research activities and applications in operational certification contexts.

5. https://cybersecuritycertcluster.eu/

EMERALD's public software, deliverables, scientific publications, showcases and other dissemination materials **will remain available through the project's online repositories and communication channels**. These resources provide practical knowledge that can be reused by cloud service providers, auditors, researchers and organisations developing new approaches to cybersecurity compliance.

Collaboration established through the **European Cluster for Cybersecurity Certification**[5] will provide an important channel for continuing exchanges with related European initiatives. Through these foundations, EMERALD's results can continue to contribute to the evolution of cloud certification and to emerging European cybersecurity and regulatory requirements.

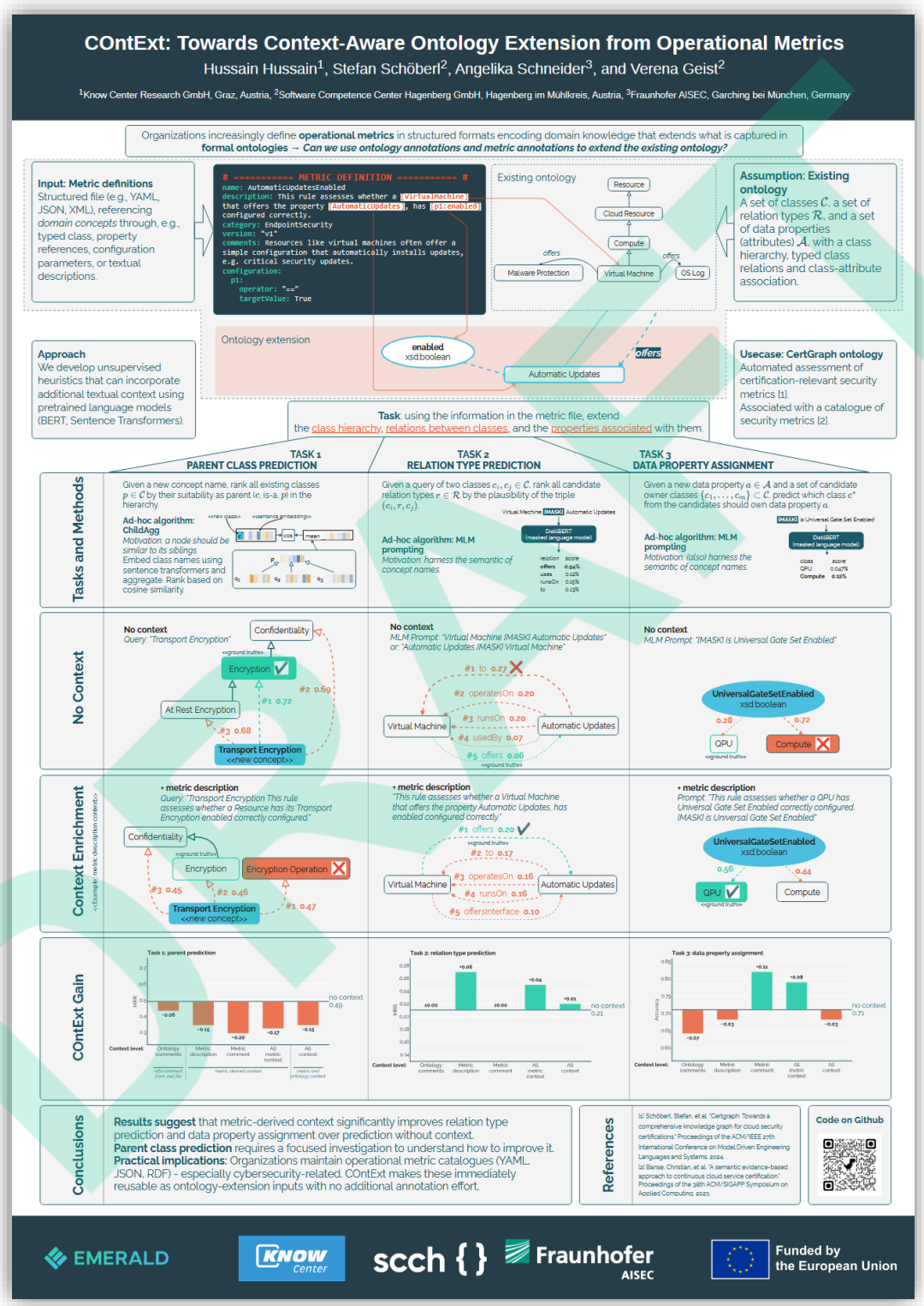


tecnalia
Fraunhofer
Fabasoft
CaixaBank
IONOS
CloudFerro
OpenNebula
DNV CYBER

CC BY-SA

APPENDIX D Posters

This section includes the fourth poster produced during the second reporting period of the project[43].



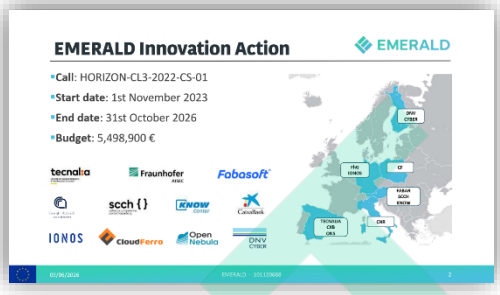
[43] https://www.emerald-he.eu/posters/

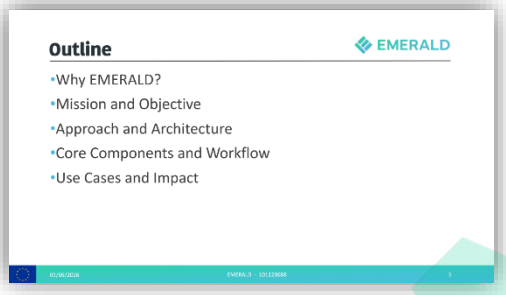
CC BY-SA

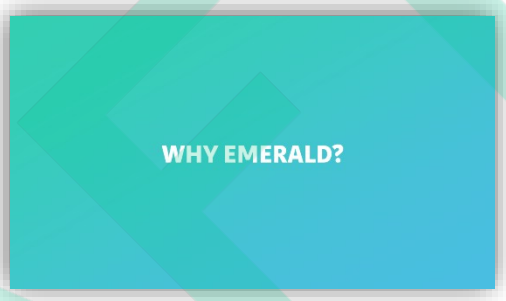
APPENDIX E Presentation

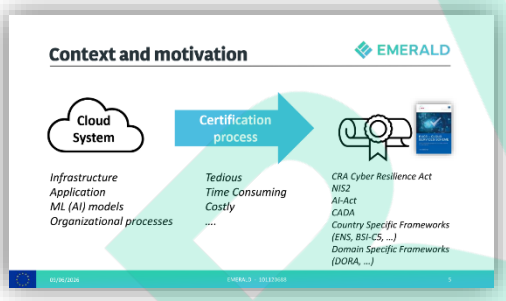
This appendix reports the second EMERALD general presentation[44].

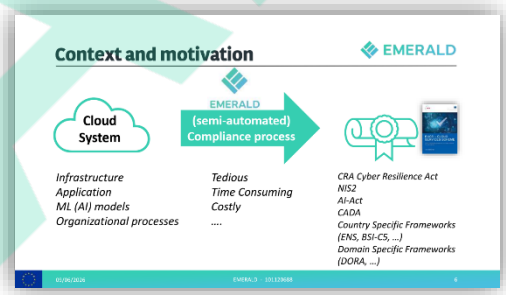










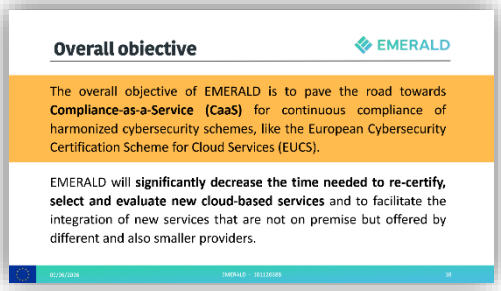


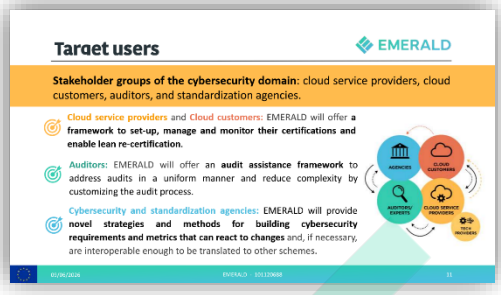


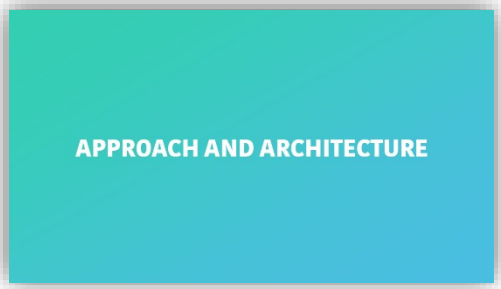


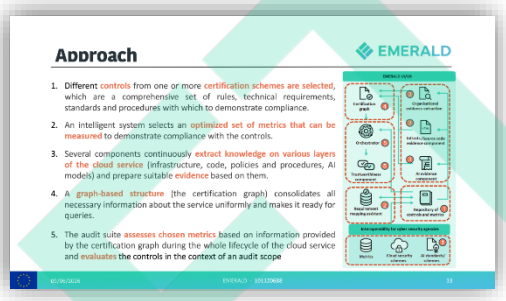
[44] https://www.emerald-he.eu/presentations/

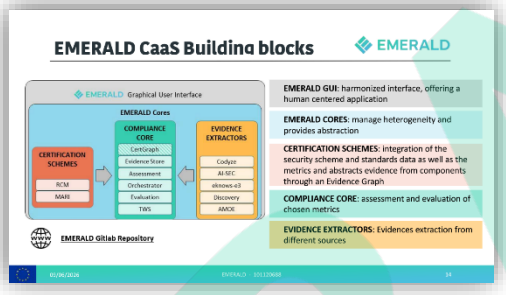
CC BY-SA

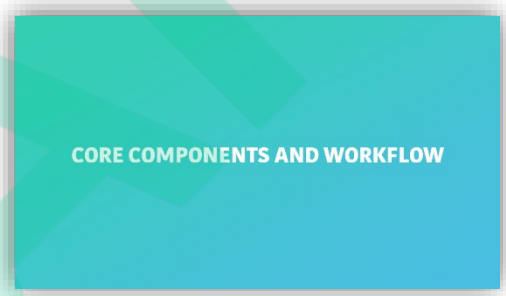

Overall objective
EMERALD
The overall objective of EMERALD is to pave the road towards Compliance-as-a-Service (CaaS) for continuous compliance of harmonized cybersecurity schemes, like the European Cybersecurity Certification Scheme for Cloud Services (EUCS).
EMERALD will significantly decrease the time needed to re-certify, select and evaluate new cloud-based services and to facilitate the integration of new services that are not on premise but offered by different and also smaller providers.

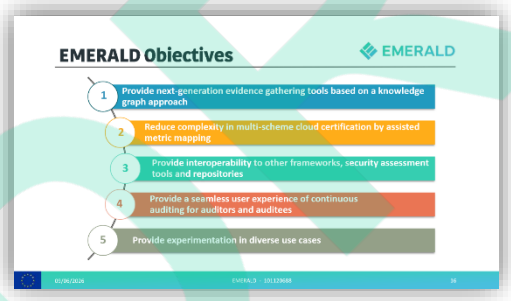

Target users
EMERALD
Stakeholder groups of the cybersecurity domain: cloud service providers, cloud customers, auditors, and standardization agencies.
Cloud service providers and Cloud customers: EMERALD will offer a framework to set-up, manage and monitor their certifications and enable lean re-certification.
Auditors: EMERALD will offer an audit assistance framework to address audits in a uniform manner and reduce complexity by customizing the audit process.
Cybersecurity and standardization agencies: EMERALD will provide novel strategies and methods for building cybersecurity requirements and metrics that can react to changes and, if necessary, are interoperable enough to be translated to other schemes.

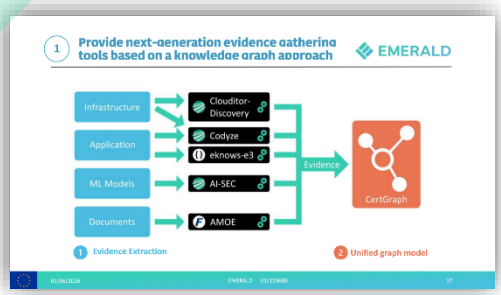

APPROACH AND ARCHITECTURE

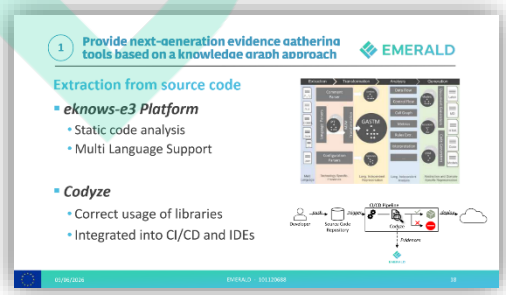

Approach
EMERALD
1. Different controls from one or more certification schemes are selected, which are a comprehensive set of rules, technical requirements, standards and procedures with which to demonstrate compliance.
2. An intelligent system selects an optimized set of metrics that can be measured to demonstrate compliance with the controls.
3. Several components continuously extract knowledge on various layers of the cloud service (infrastructure, code, policies and procedures, AI models) and prepare suitable evidence based on them.
4. A graph-based structure (the certification graph) consolidates all necessary information about the service uniformly and makes it ready for queries.
5. The audit suite assesses chosen metrics based on information provided by the certification graph during the whole lifecycle of the cloud service and evaluates the controls in the context of an audit scope

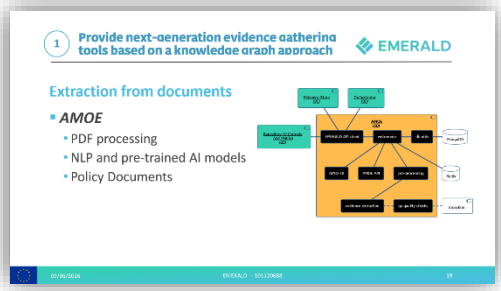

EMERALD CaaS Building blocks
EMERALD
EMERALD Graphical User Interface
EMERALD Cores
COMPLIANCE CORE
CertGraph
Evidence Store
Assessment
Orchestrator
Evaluation
TIRS
CERTIFICATION SCHEMES
RCM
MAR
EVIDENCE EXTRACTORS
Codyze
AI-SEC
eknows-e3
Discovery
AMOE
EMERALD GUI: harmonized interface, offering a human centered application
EMERALD CORES: manage heterogeneity and provides abstraction
CERTIFICATION SCHEMES: integration of the security scheme and standards data as well as the metrics and abstracts evidence from components through an Evidence Graph
COMPLIANCE CORE: assessment and evaluation of chosen metrics
EVIDENCE EXTRACTORS: Evidences extraction from different sources
EMERALD GitLab Repository


CORE COMPONENTS AND WORKFLOW

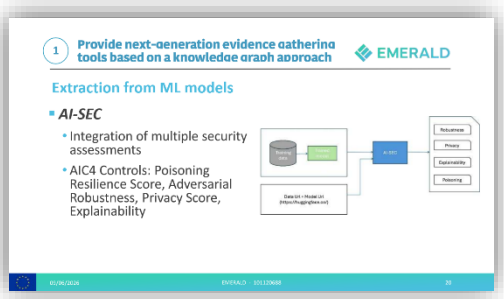

EMERALD Objectives
EMERALD
1 Provide next-generation evidence gathering tools based on a knowledge graph approach
2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping
3 Provide interoperability to other frameworks, security assessment tools and repositories
4 Provide a seamless user experience of continuous auditing for auditors and auditees
5 Provide experimentation in diverse use cases

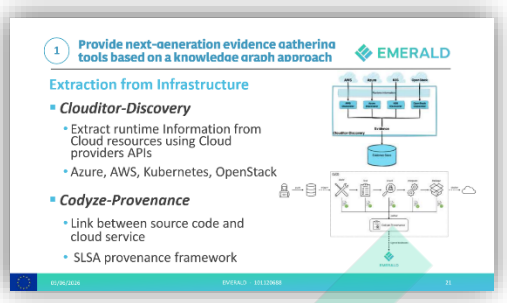

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Infrastructure
Application
ML Models
Documents
Cloudtor-Discovery
Codyze
eknows-e3
AI-SEC
AMOE
Evidence
CertGraph
1 Evidence Extraction
2 Unified graph model

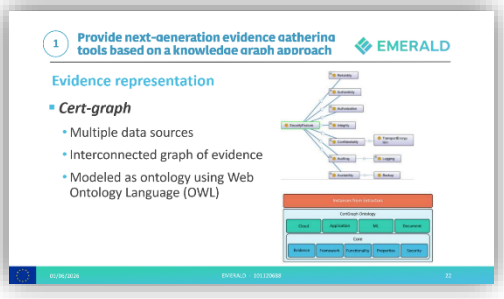

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Extraction from source code
eknows-e3 Platform
Static code analysis
Multi Language Support
Codyze
Correct usage of libraries
Integrated into CI/CD and IDEs

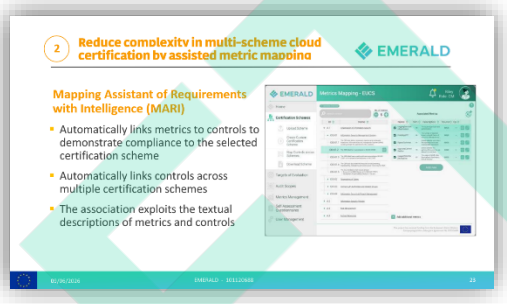

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Extraction from documents
AMOE
PDF processing
NLP and pre-trained AI models
Policy Documents

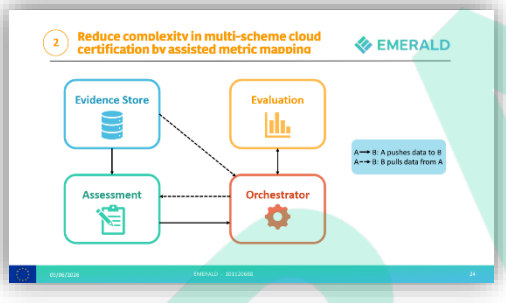
CC BY-SA

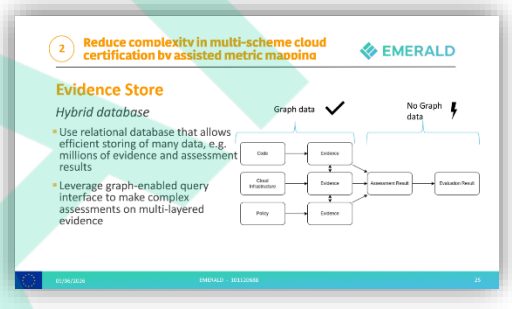

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Extraction from ML models
AI-SEC
Integration of multiple security assessments
AIC4 Controls: Poisoning Resilience Score, Adversarial Robustness, Privacy Score, Explainability

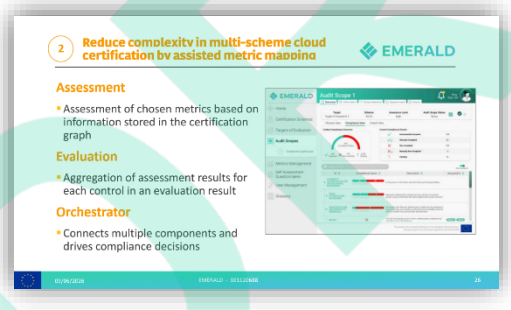

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Extraction from Infrastructure
Clouditor-Discovery
Extract runtime Information from Cloud resources using Cloud providers APIs
Azure, AWS, Kubernetes, OpenStack
Codyze-Provenance
Link between source code and cloud service
SLSA provenance framework

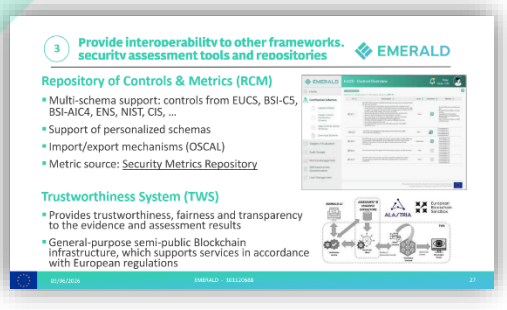

1 Provide next-generation evidence gathering tools based on a knowledge graph approach
EMERALD
Evidence representation
Cert-graph
Multiple data sources
Interconnected graph of evidence
Modeled as ontology using Web Ontology Language (OWL)


2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping
EMERALD
Mapping Assistant of Requirements with Intelligence (MARI)
Automatically links metrics to controls to demonstrate compliance to the selected certification scheme
Automatically links controls across multiple certification schemes
The association exploits the textual descriptions of metrics and controls

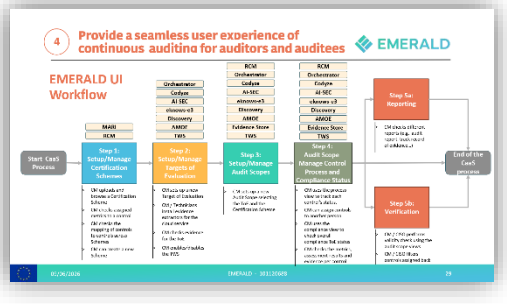

2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping
EMERALD
Evidence Store
Evaluation
Assessment
Orchestrator
A → B: A pushes data to B
A ← B: B pulls data from A


2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping
EMERALD
Evidence Store
Hybrid database
Use relational database that allows efficient storing of many data, e.g. millions of evidence and assessment results
Leverage graph-enabled query interface to make complex assessments on multi-layered evidence
Graph data
No Graph data

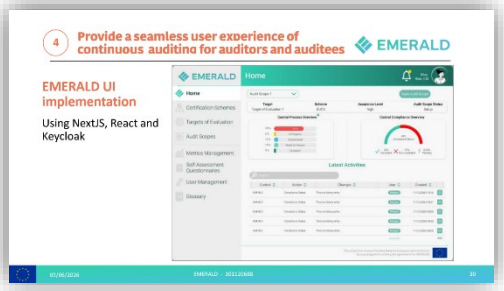

2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping
EMERALD
Assessment
Assessment of chosen metrics based on information stored in the certification graph
Evaluation
Aggregation of assessment results for each control in an evaluation result
Orchestrator
Connects multiple components and drives compliance decisions

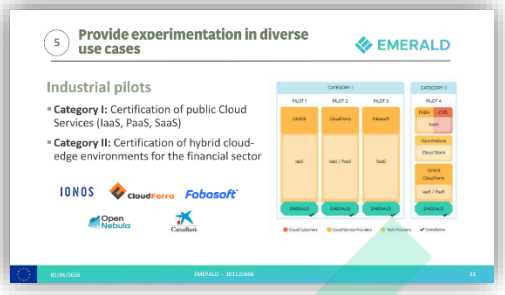

3 Provide interoperability to other frameworks, security assessment tools and repositories
EMERALD
Repository of Controls & Metrics (RCM)
Multi-schema support: controls from EUCS, BSI-C5, BSI-AIC4, ENS, NIST, CIS, ...
Support of personalized schemas
Import/export mechanisms (OSCAL)
Metric source: Security Metrics Repository
Trustworthiness System (TWS)
Provides trustworthiness, fairness and transparency to the evidence and assessment results
General-purpose semi-public Blockchain infrastructure, which supports services in accordance with European regulations


4 Provide a seamless user experience of continuous auditing for auditors and auditees
EMERALD
EMERALD UI/UX
User interaction concept and conducted studies to show what information each user needs in an audit process
User-centered requirements
7 Personas divided into 3 stakeholder groups
Work process modelling: scenarios and user journeys to define interactions
UI/UX design: Created paper and clickable mock-ups through iterative co-design
The Compliance Manager

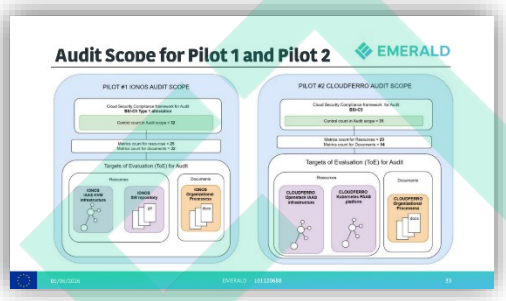

4 Provide a seamless user experience of continuous auditing for auditors and auditees
EMERALD
EMERALD UI Workflow
Start: CaaS Process
Step 1: Setup/Manage Certification Schemes
Step 2: Setup/Manage Targets of Evaluation
Step 3: Setup/Manage Audit Scopes
Step 4: Audit Scope Manage Control Process and Continuous Audits
Step 4a: Reporting
Step 4b: Verification
End of the CaaS process

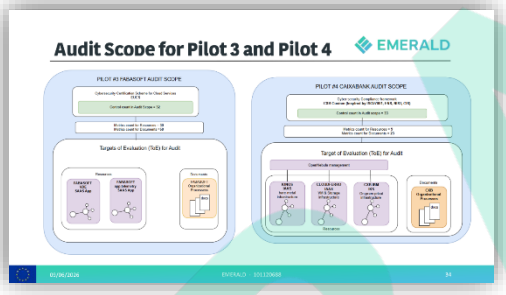
(cc) BY-SA

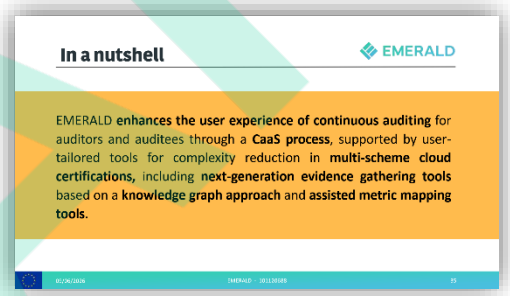

4 Provide a seamless user experience of continuous auditing for auditors and auditees
EMERALD
EMERALD UI implementation
Using NextJS, React and Keycloak

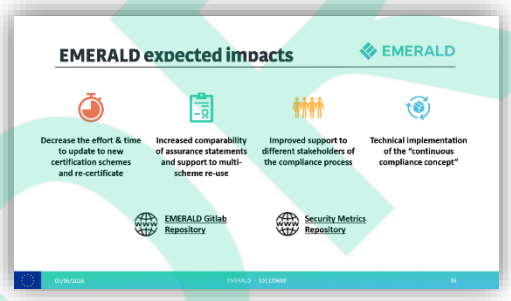

5 Provide experimentation in diverse use cases
EMERALD
Industrial pilots
Category I: Certification of public Cloud Services (IaaS, PaaS, SaaS)
Category II: Certification of hybrid cloud-edge environments for the financial sector
IONOS
CloudFerro
Fabasoft
OpenNebula


USE CASES AND IMPACT


Audit Scope for Pilot 1 and Pilot 2
EMERALD


Audit Scope for Pilot 3 and Pilot 4
EMERALD


In a nutshell
EMERALD
EMERALD enhances the user experience of continuous auditing for auditors and auditees through a CaaS process, supported by user-tailored tools for complexity reduction in multi-scheme cloud certifications, including next-generation evidence gathering tools based on a knowledge graph approach and assisted metric mapping tools.


EMERALD expected impacts
EMERALD
Decrease the effort & time to update to new certification schemes and re-certificate
Increased comparability of assurance statements and support to multi-scheme re-use
Improved support to different stakeholders of the compliance process
Technical implementation of the "continuous compliance concept"
EMERALD Gitlab Repository
Security Metrics Repository


www.emerald-he.eu
@emerald-he-project
emerald-he-project
Scan me!

(cc) BY-SA