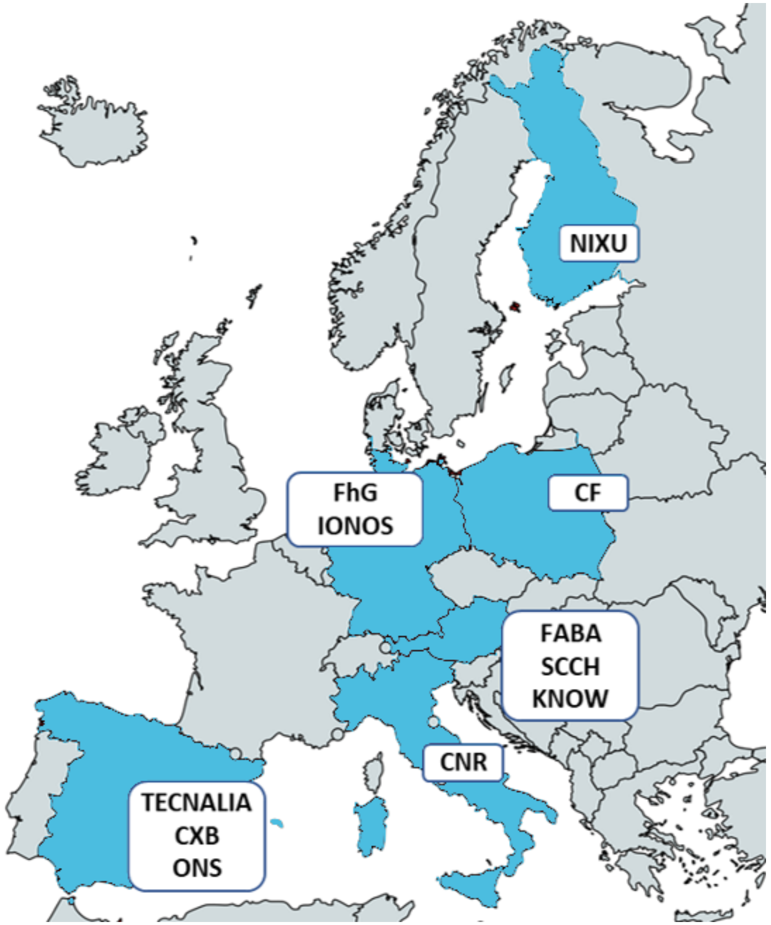
EMERALD

Evidence Management for Continuous Certification as a Service in the Cloud

This project has received funding from the European Union’s Horizon Europe programme under grant agreement No 101120688

EMERALD Innovation Action

- **Call**: HORIZON-CL3-2022-CS-01
- **Start date**: 1st November 2023
- **End date**: 31st October 2026
- **Budget**: 5,498,900 €



EMERALD Mission

EMERALD

- EMERALD **leverages the findings** of the well esteemed H2020 project MEDINA (GA 952633), starting from TRL 5 in summer 2023 and advances them in the EMERALD Core to TRL 7.
- EMERALD **will focus on evidence management components** for the continuous certification approach.
- EMERALD **will provide a proof of concept** (PoC) for mapping the findings to future Artificial Intelligence (AI) certification schemes.

MEDINA

EU
CYBERSECURITY
CERTIFICATION

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

AI Services

AI Cloud Service Compliance
Criteria Catalogue (AIC4)

Deutschland
Digital•Sicher•BSI•

EMERALD Overall objective

The main objective of EMERALD is to pave the road towards **Certification-as-a-Service (CaaS)** for continuous certification of harmonized cybersecurity schemes, like the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

EMERALD Main objectives

EMERALD

- Provide next-generation evidence gathering tools based on a **knowledge graph approach**
- Reduce complexity in **multi-scheme Cloud certifications** by assisted metric mapping
- Provide a **seamless user experience** of continuous auditing for auditors and auditees
- Provide **interoperability to other frameworks**, security assessment tools and repositories
- Validate the outcomes in **industrial pilots**
- **Promote** the project, **disseminate** results and **coordinate** with international agencies

EMERALD Key Results 1/3

EMERALD

KR1: EXTRACT

Evidence extraction from cloud service: A framework to continuously extract knowledge on various layers of the cloud service and prepare suitable evidence based on them. This result covers the improvements on existing evidence extraction tools and concepts of MEDINA, such as AMOE (Assessment and Management of Organisational Evidence). The framework works on utilizing information and verifies the implementation of technical and organisational measures. The tools enable different levels of abstraction – from low level such as source code to higher levels, such as policies and procedures.

KR2: CERTGRAPH

Certification graph: A graph-based structure, the certification graph, to consolidate all necessary information of the service and make it easily query-able. The graph-based approach allows storing and linking heterogeneous information extracted from different evidence sources. Furthermore, linking allows to create additional nodes in the graph that aggregate individual aspects and fragments of information to a higher-level of combined evidence, while maintaining traceability back to information sources.

KR3: OPTIMA

Optimized metric selection: An intelligent system to select an optimized set of metrics that can be measured to demonstrate compliance to the selected certification scheme. One of such optimizations could be the maximum amount of re-used evidence.

EMERALD Key Results 2/3

KR4: MULTICERT

Cloud certifications: A tool to assess chosen metrics based on information stored in the certification graph and to evaluate the final certificate decision.

KR5: AIPOC

Proof of Concept for AI-based certifications: By transferring the innovation results to upcoming AI certification schemes, EMERALD establishes a Proof of Concept (PoC) on how to scale the Certification as a Service (CaaS) approach to cloud-based AI systems.

KR6: EMERALD UI/UX

User experience for complexity reduction: A user interaction concept and conducted studies to show what information each user needs in an audit process. The concept shall lead to a user interface (UI), which is tailored to the users’ needs during all stages of an audit and guides them through the process of identifying problems top down – from high level requirements down to specific implementation in documents (e.g., policies) or technical specifications.

EMERALD Key Results 3/3

KR7: INTEROP

Interoperable assessment, evidence and catalogue data: EMERALD will provide an interoperability layer among the trustworthy systems, assessment results and catalogue data. Security schemes are prone to change and thus updates would be required. EMERALD aims to mitigate this by incorporating the scheme data in a standardized format such as OSCAL (Open Security Controls Assessment Language). Furthermore, EMERALD aims at providing interoperability at the trustworthy evidence layer by evaluating usage of the European Blockchain Services Infrastructure (EBSI) for its trustworthiness system.

KR8: PILOTS

Industrial pilots: Involvement of realistic use cases by potential applicants of EMERALD. This is key to derive and validate the proposed contents of the project objectives. PILOTS is responsible for providing these real-world application examples and test data. The data will be forwarded to the evidence extraction stakeholders, so the components can be fine-tuned to improve quality of the results.

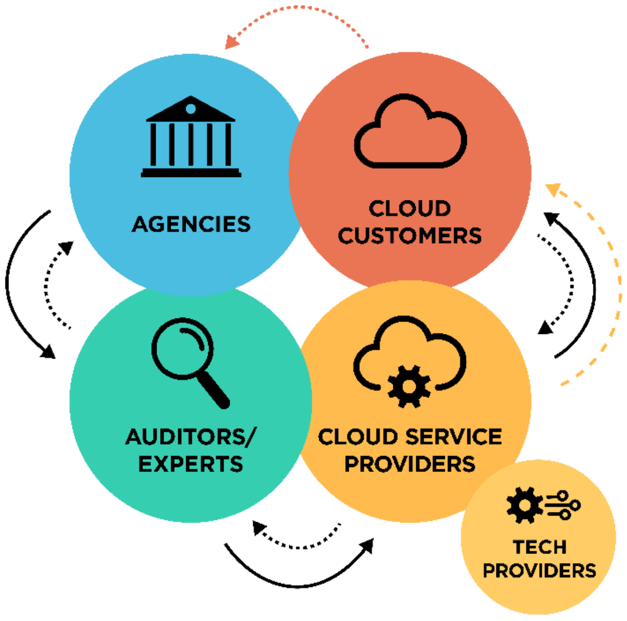
KR9: DECAS

Dissemination, exploitation, communication and standardization: Dissemination and communication of the project results via multiple channels, relevant conferences (e.g., ETSI security conference) and the scientific community. Exploitation of the project achievements by the technical and pilot partners. Standardization activities to discuss, verify and deepen the project findings with standardization bodies. Concepts for continuous use and deployment after the project has finished need to be prepared and documented.

EMERALD Target users

Addressed users are stakeholder groups of the cybersecurity domain: cloud service providers, cloud customers, auditors, and standardization agencies.

- For cloud service providers as well as cloud customers, EMERALD will offer **a framework to set-up, manage and monitor their certifications and enable lean re-certification**.
- For auditors, EMERALD will be an **audit assistance framework**.
- For 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.

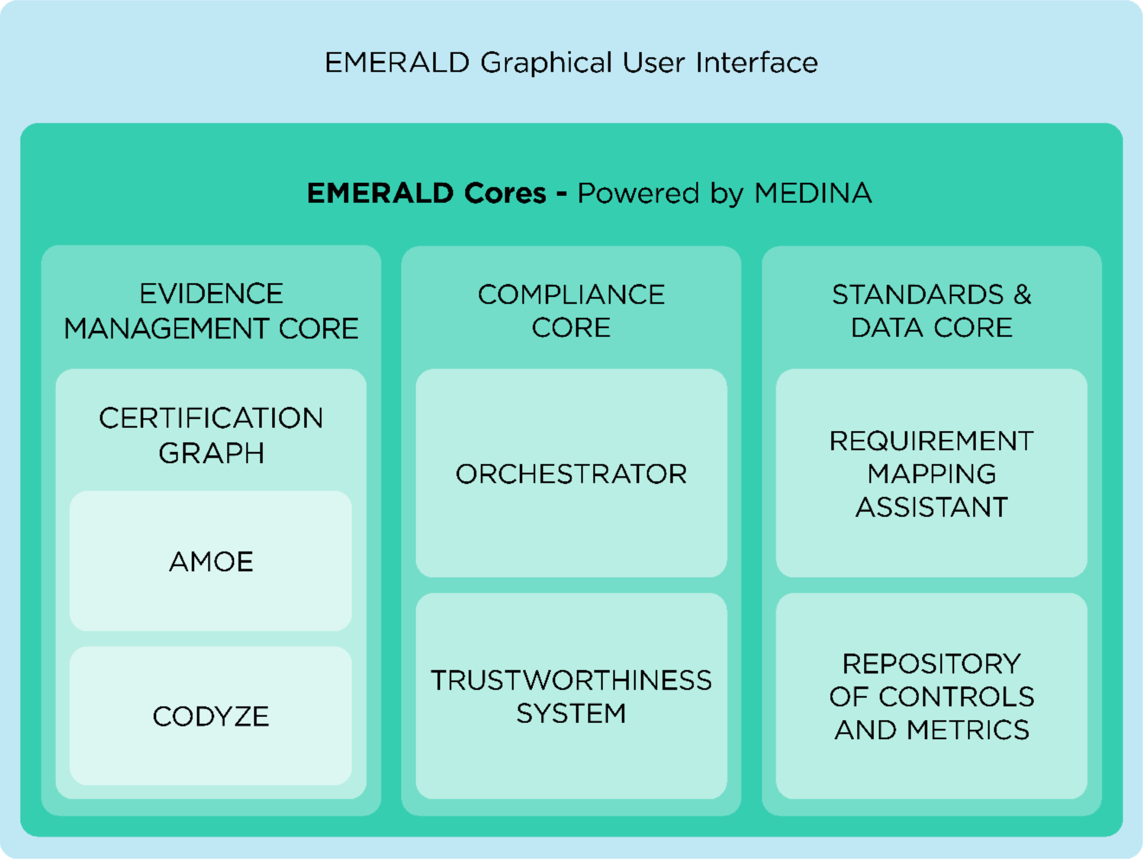


● Stakeholder of the cybersecurity domain and EMERALD
— Supplier relationship
······ Costomer relationship
- - - Certification mandatory for bussiness decisions
······ Demand security schemes to build up trust in cloud services

EMERALD Framework

To achieve the overall objective, EMERALD will design and implement a **user interaction concept**, offering a uniform way to address audits and offer the previously mentioned stakeholders a solid degree of complexity reduction through the customization of the audit process.

EMERALD Overview



EMERALD Graphical User Interface

EMERALD Cores - Powered by MEDINA

EVIDENCE MANAGEMENT CORE

CERTIFICATION GRAPH

AMOE

CODYZE

COMPLIANCE CORE

ORCHESTRATOR

TRUSTWORTHINESS SYSTEM

STANDARDS & DATA CORE

REQUIREMENT MAPPING ASSISTANT

REPOSITORY OF CONTROLS AND METRICS

EMERALD GUI: harmonized interface, offering a human centered application

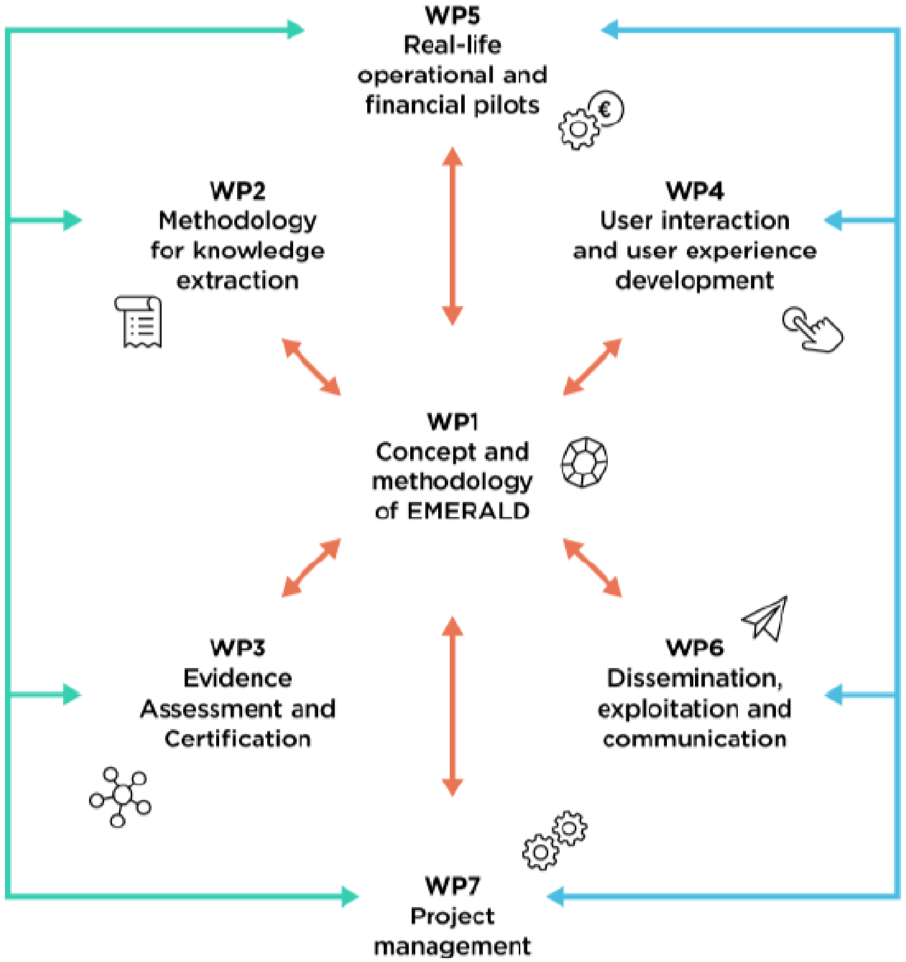
EMERALD CORE: manages heterogeneity and provides abstraction

EVIDENCE MANAGEMENT CORE: abstracts evidence from components through an Evidence Graph

COMPLIANCE CORE: assessment and evaluation of chosen metrics

STANDARDS & DATA CORE: integration of the security scheme and standards data as well as the metrics

EMERALD Work Packages



WP5
Real-life operational and financial pilots

WP2
Methodology for knowledge extraction

WP4
User interaction and user experience development

WP1
Concept and methodology of EMERALD

WP3
Evidence Assessment and Certification

WP6
Dissemination, exploitation and communication

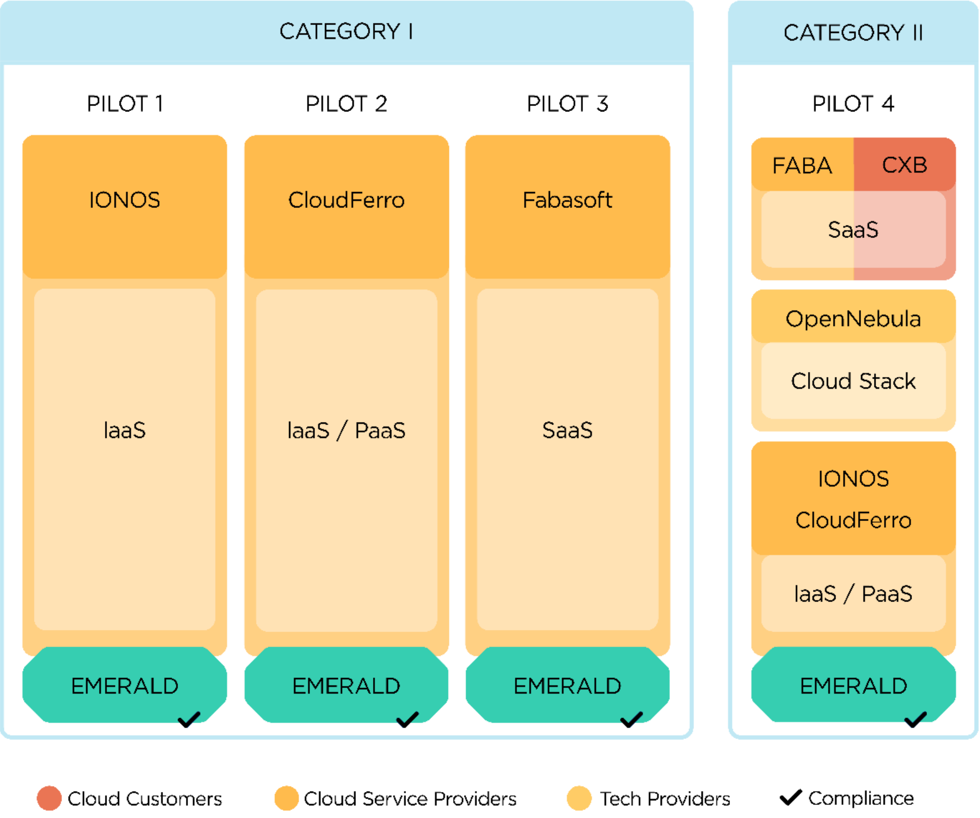
WP7
Project management

EMERALD Industrial pilots

Involvement of realistic use cases by potential applicants of EMERALD.

Category I: Certification of public Cloud Services (IaaS, PaaS, SaaS)

Category II: Certification of hybrid cloud-edge environments for the financial sector



CATEGORY I			CATEGORY II
PILOT 1	PILOT 2	PILOT 3	PILOT 4
IONOS	CloudFerro	Fabasoft	FABA CXB SaaS OpenNebula Cloud Stack IONOS CloudFerro IaaS / PaaS
IaaS	IaaS / PaaS	SaaS	
EMERALD ✓	EMERALD ✓	EMERALD ✓	EMERALD ✓

● Cloud Customers ● Cloud Service Providers ● Tech Providers ✓ Compliance

More information

Further details are available at

- **EMERALD website**

  www.emerald-he.eu

- **X**

  EmeraldHEproj

- **LinkedIn**

  emerald-he-project

EVIDENCE MANAGEMENT FOR CONTINUOUS CERTIFICATION
AS A SERVICE IN THE CLOUD

EMERALD

Thank you!