EMERALD

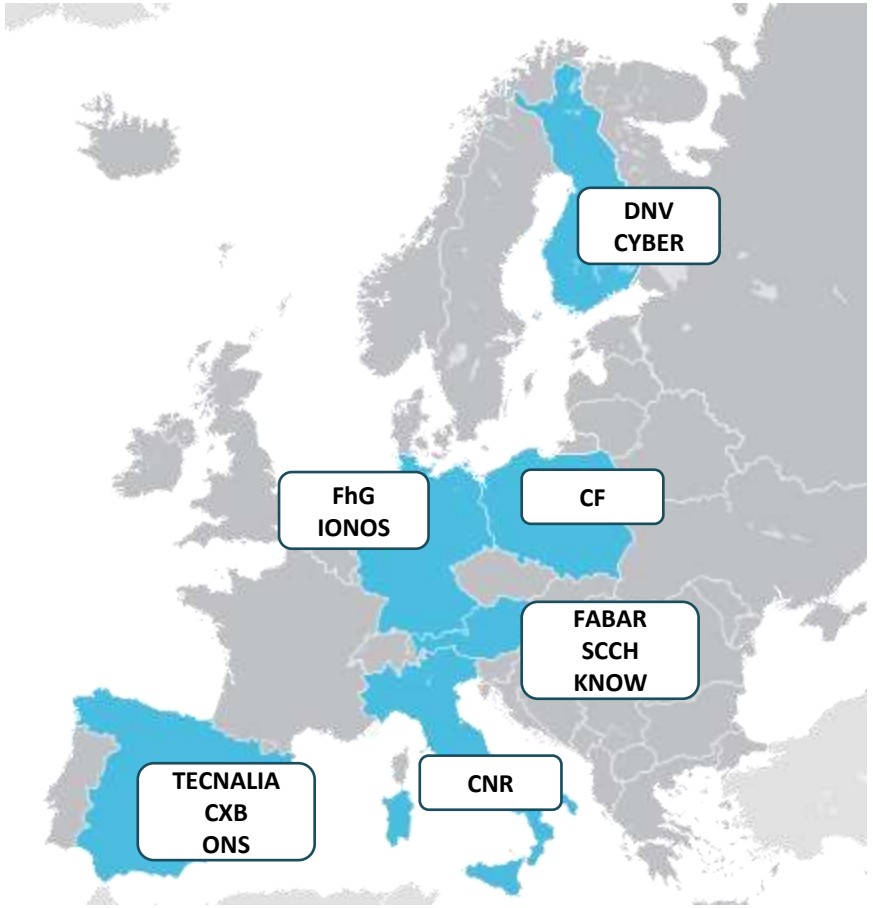
EMERALD EU Project

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 €

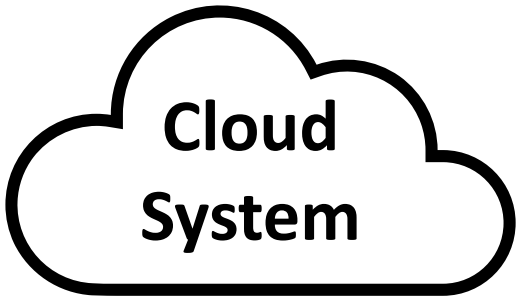


Outline

- Why EMERALD?
- Mission and Objective
- Approach and Architecture
- Core Components and Workflow
- Use Cases and Impact

WHY EMERALD?

Context and motivation



Infrastructure
Application
ML (AI) models
Organizational processes

Tedious
Time Consuming
Costly
….

CRA Cyber Resilience Act
NIS2
AI-Act
CADA
Country Specific Frameworks (ENS, BSI-C5, …)
Domain Specific Frameworks (DORA, …)

Context and motivation

Cloud System

EMERALD

(semi-automated) Compliance process

Infrastructure
Application
ML (AI) models
Organizational processes

Tedious
Time Consuming
Costly
….

CRA Cyber Resilience Act
NIS2
AI-Act
CADA
Country Specific Frameworks (ENS, BSI-C5, …)
Domain Specific Frameworks (DORA, …)

Driving the CaaS Vision

To bring Cloud certification into the future, **complexity must be reduced** for all stakeholders. This can be **achieved through** a **Compliance-as-a-Service (CaaS)** approach. By introducing a **user-centric and guided workflow process**, which is combined to the monitoring of the system-state-compliance, EMERALD addresses this need, providing advanced **tools for automated evidence management and metrics mapping**.

MISSION AND OBJECTIVE

EMERALD Mission

- Make cloud **certification simpler, faster, and more efficient** for all stakeholders
- Build on **H2020 MEDINA results**, advancing to **semi-automated compliance**
- Focus on **evidence management** for continuous compliance
- Support alignment with **multiple cybersecurity standards**
- Provide **proof of concept for future AI** certification schemes

MEDINA

EU CYBERSECURITY CERTIFICATION

enisa

AI Services

AI Cloud Service Compliance Criteria Catalogue (AIC4)

Deutschland Digital·Sicher·BSI·

Overall objective

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

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**.

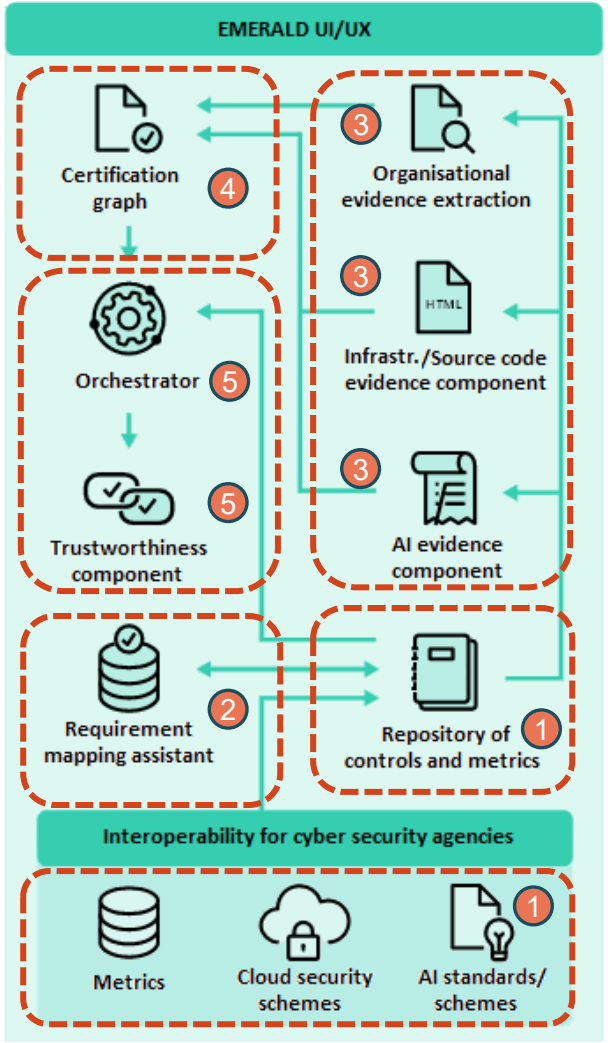
Auditors: EMERALD will offer an **audit assistance framework** to address audits in a uniform manner and reduce complexity by customizing the audit process.

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.

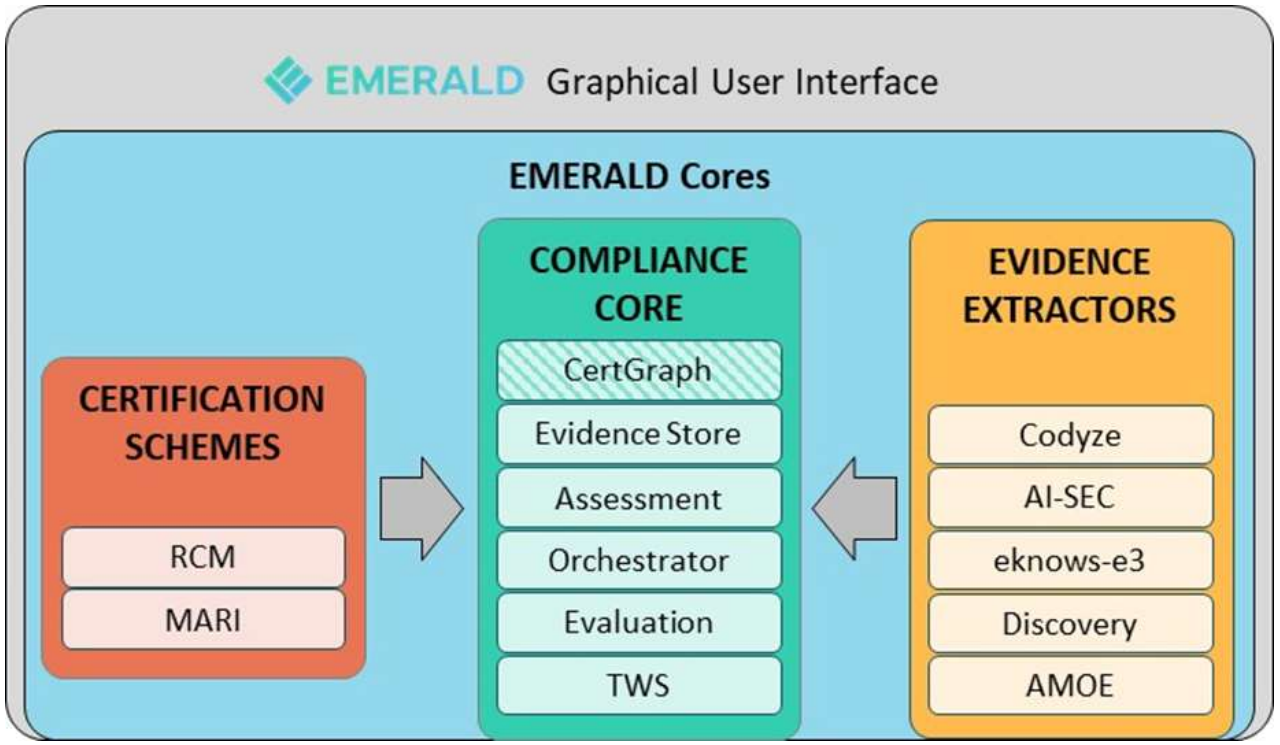
APPROACH AND ARCHITECTURE

Approach

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 Gitlab Repository

EMERALD GUI: harmonized interface, offering a human centered application

EMERALD CORES: manage heterogeneity and provides abstraction

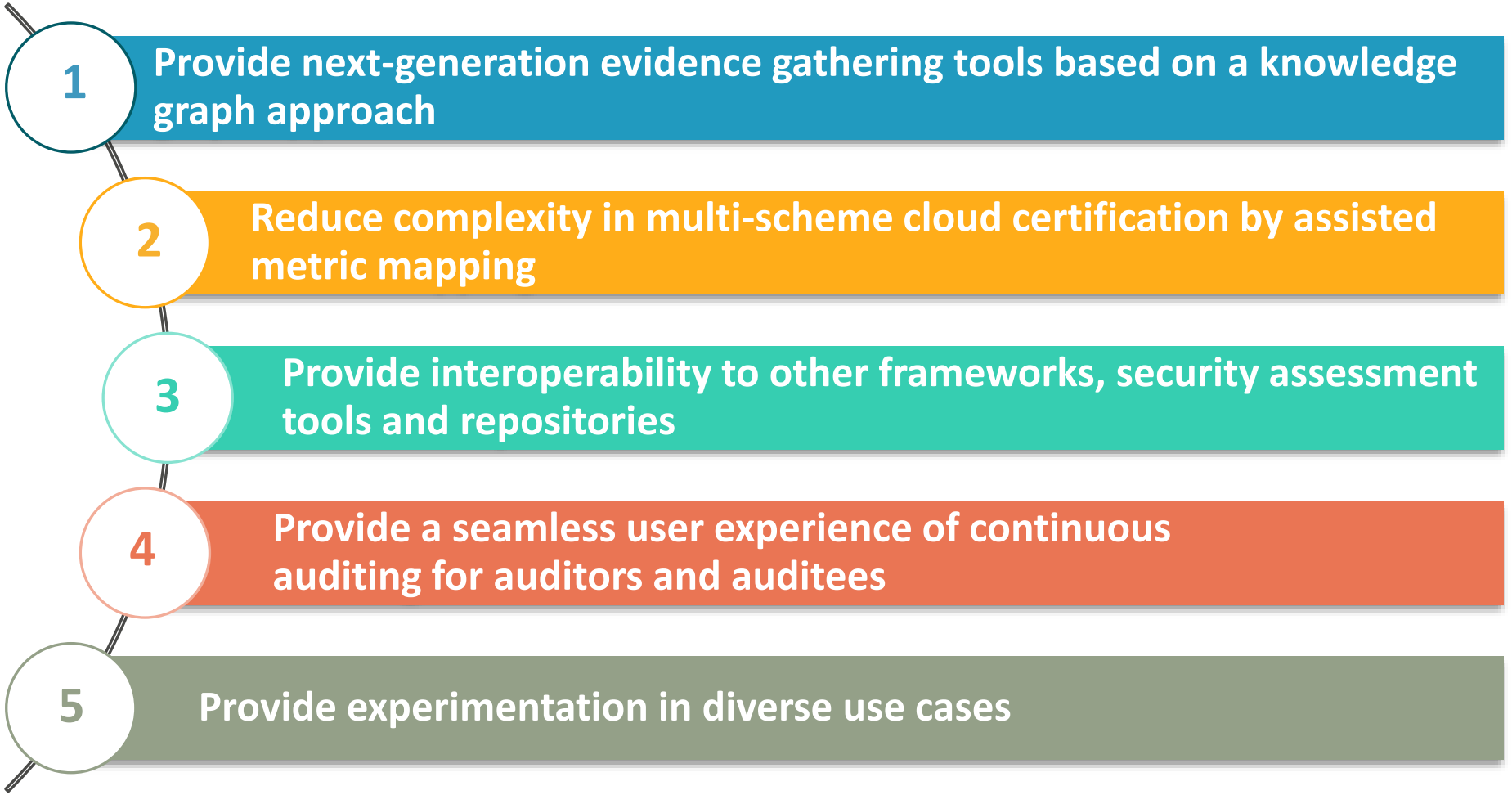
CERTIFICATION SCHEMES: integration of the security scheme and standards data as well as the metrics and abstracts evidence from components through an Evidence Graph

COMPLIANCE CORE: assessment and evaluation of chosen metrics

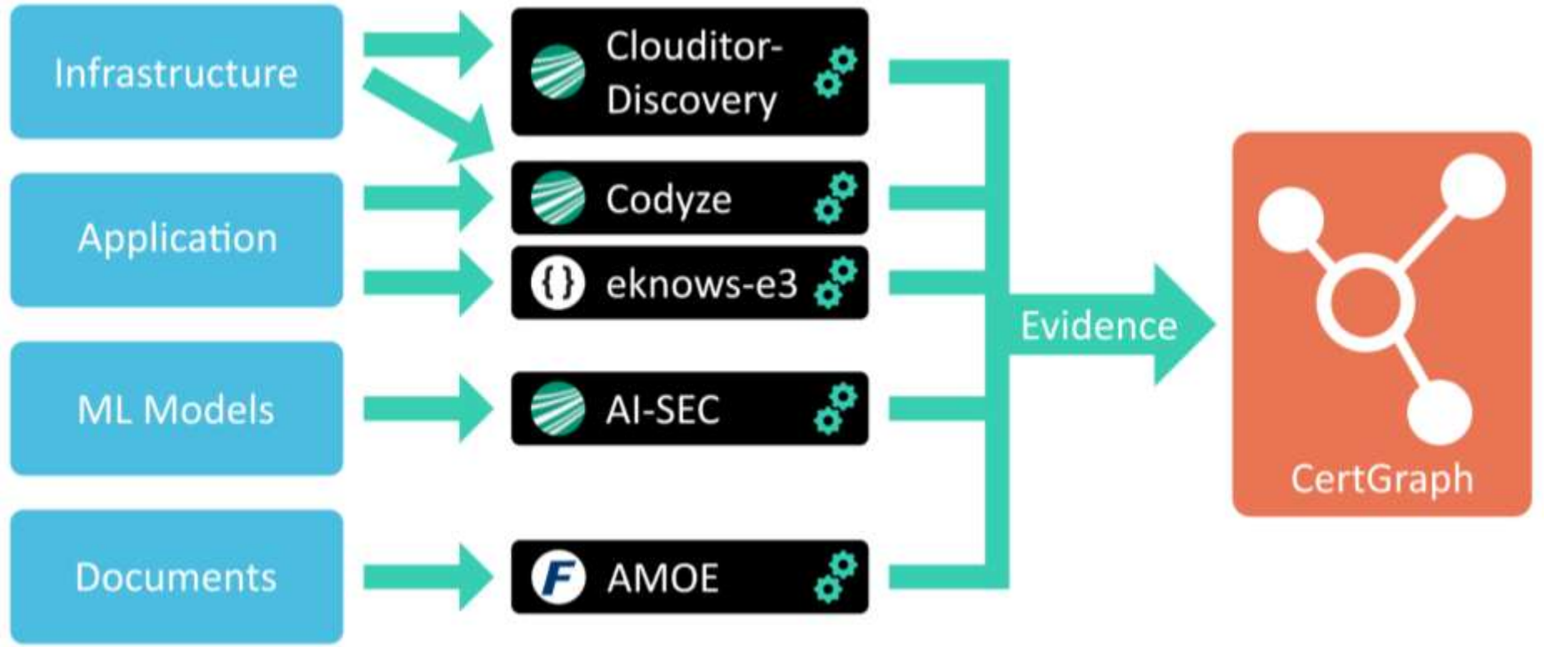
EVIDENCE EXTRACTORS: Evidences extraction from different sources

CORE COMPONENTS AND WORKFLOW

EMERALD Objectives



1 Provide next-generation evidence gathering tools based on a knowledge graph approach



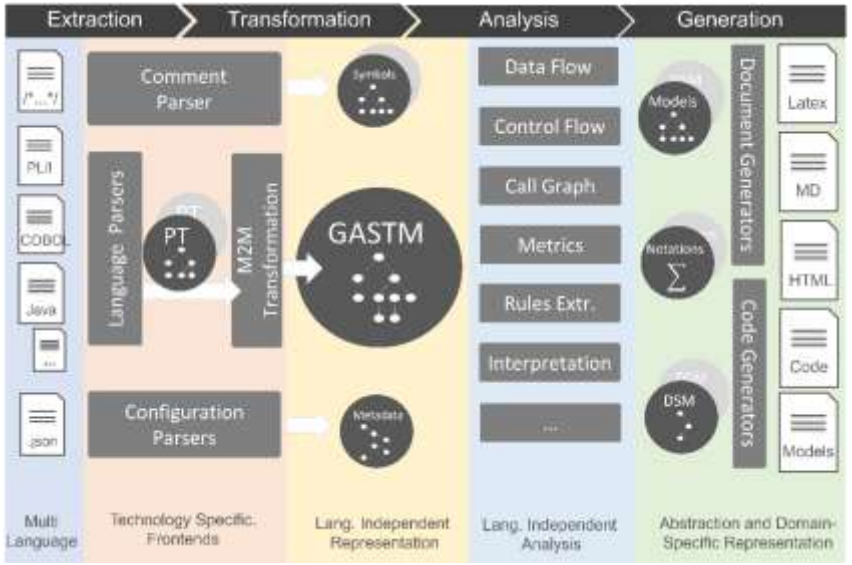
1 Evidence Extraction

2 Unified graph model

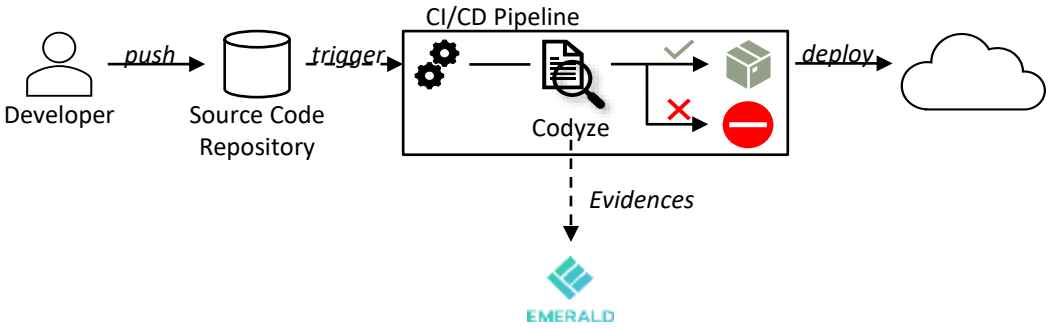
1 Provide next-generation evidence gathering tools based on a knowledge graph approach

Extraction from source code

- ***eknows-e3 Platform***
  - Static code analysis
  - Multi Language Support

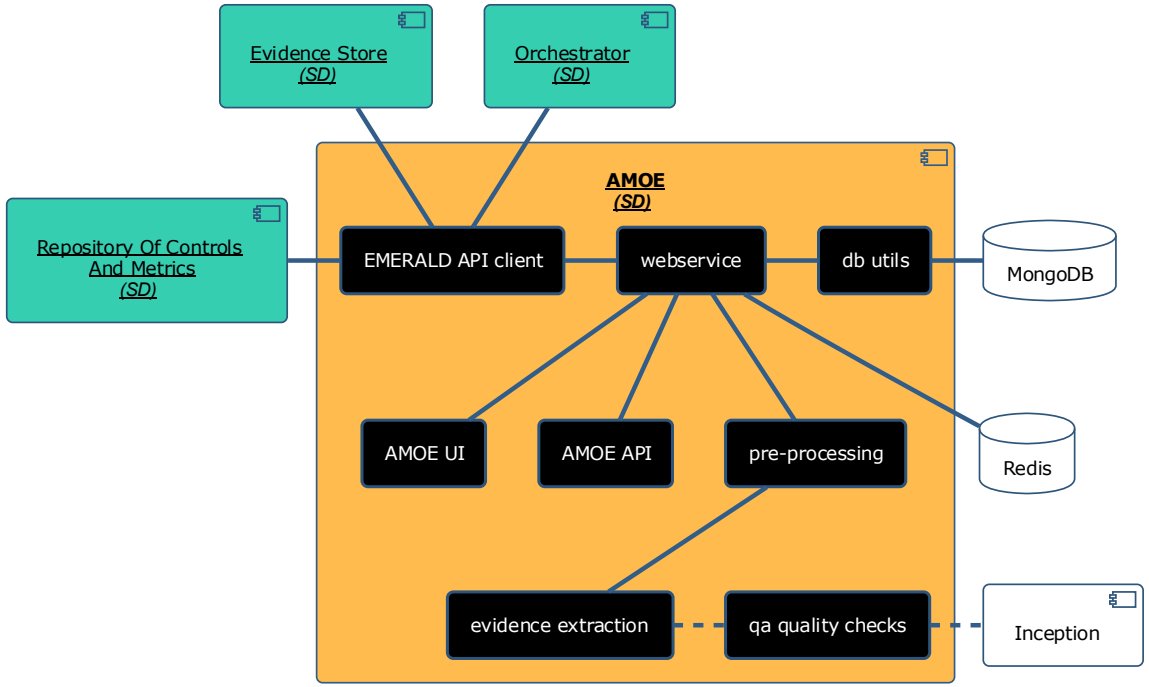


- ***Codyze***
  - Correct usage of libraries
  - Integrated into CI/CD and IDEs



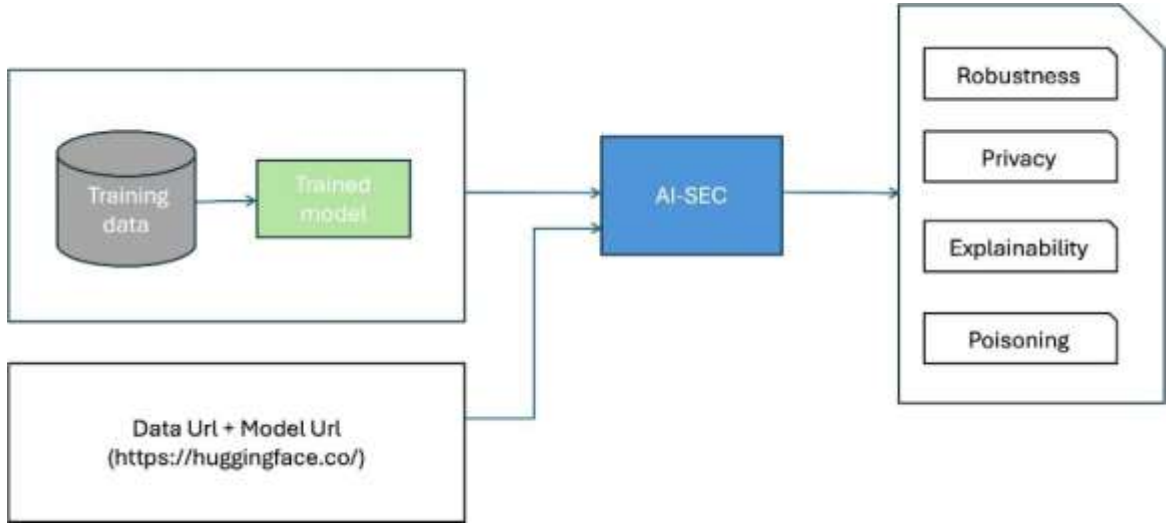
Extraction from documents

- ***AMOE***
  - PDF processing
  - NLP and pre-trained AI models
  - Policy Documents



Extraction from ML models

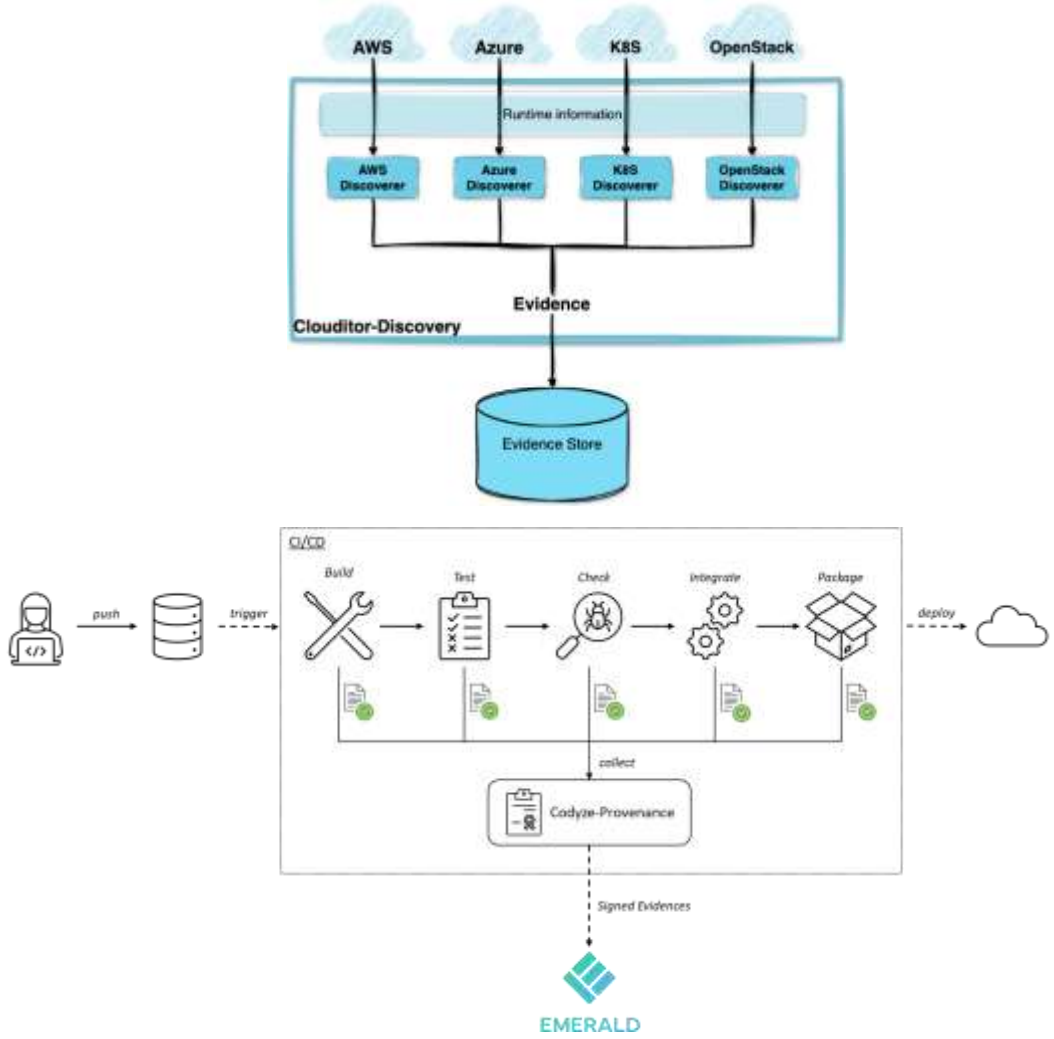
- ***AI-SEC***
  - Integration of multiple security assessments
  - AIC4 Controls: Poisoning Resilience Score, Adversarial Robustness, Privacy Score, Explainability



1 Provide next-generation evidence gathering tools based on a knowledge graph approach

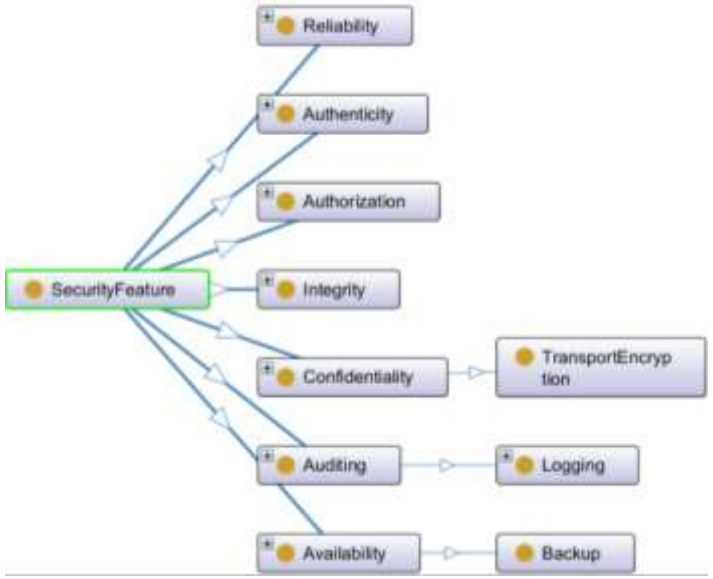
Extraction from Infrastructure

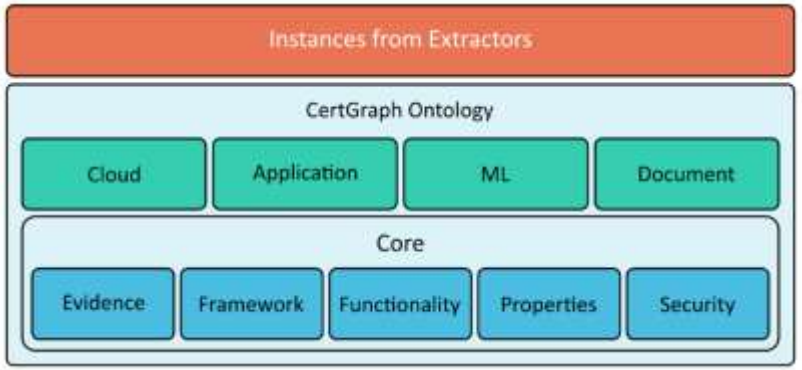
- ***Clouditor-Discovery***
  - Extract runtime Information from Cloud resources using Cloud providers APIs
  - Azure, AWS, Kubernetes, OpenStack
- ***Codyze-Provenance***
  - Link between source code and cloud service
  - SLSA provenance framework



Evidence representation

- ***Cert-graph***
  - Multiple data sources
  - Interconnected graph of evidence
  - Modeled as ontology using Web Ontology Language (OWL)

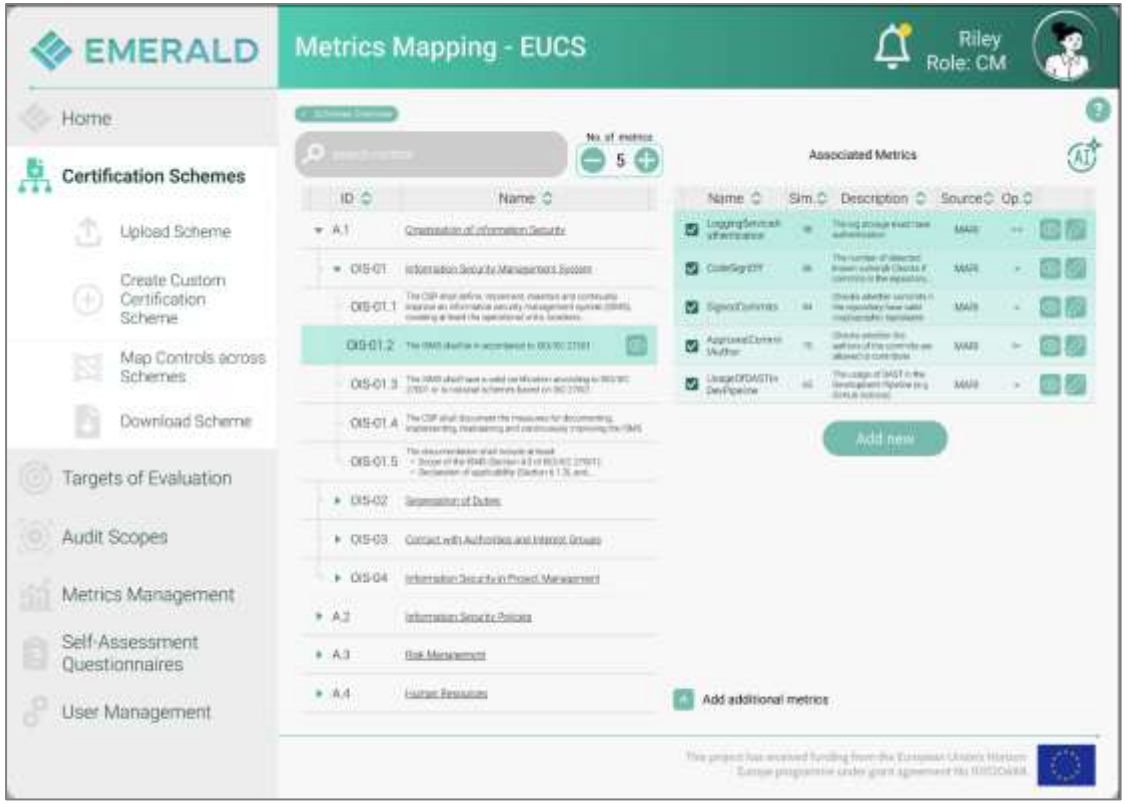




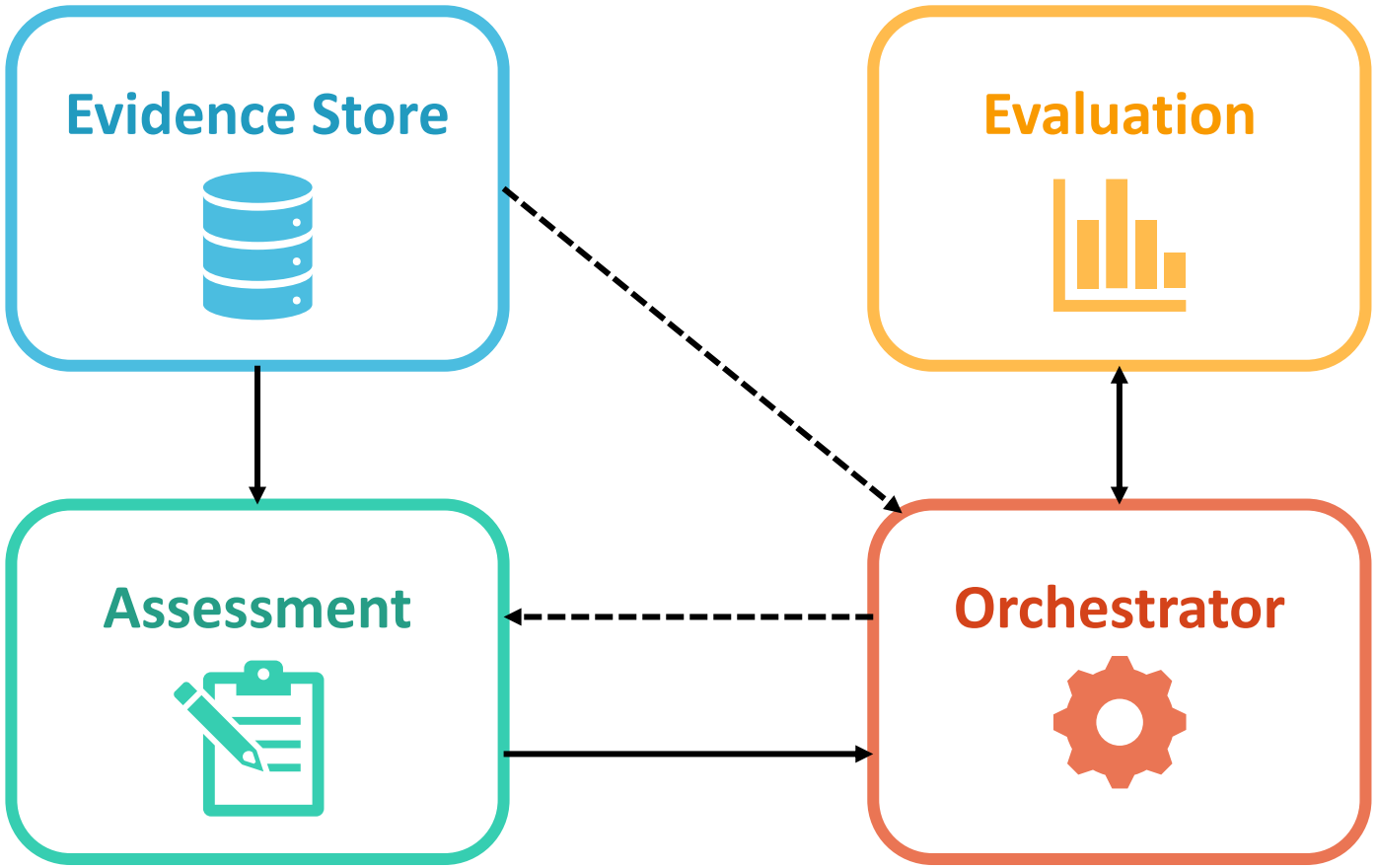
2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping

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

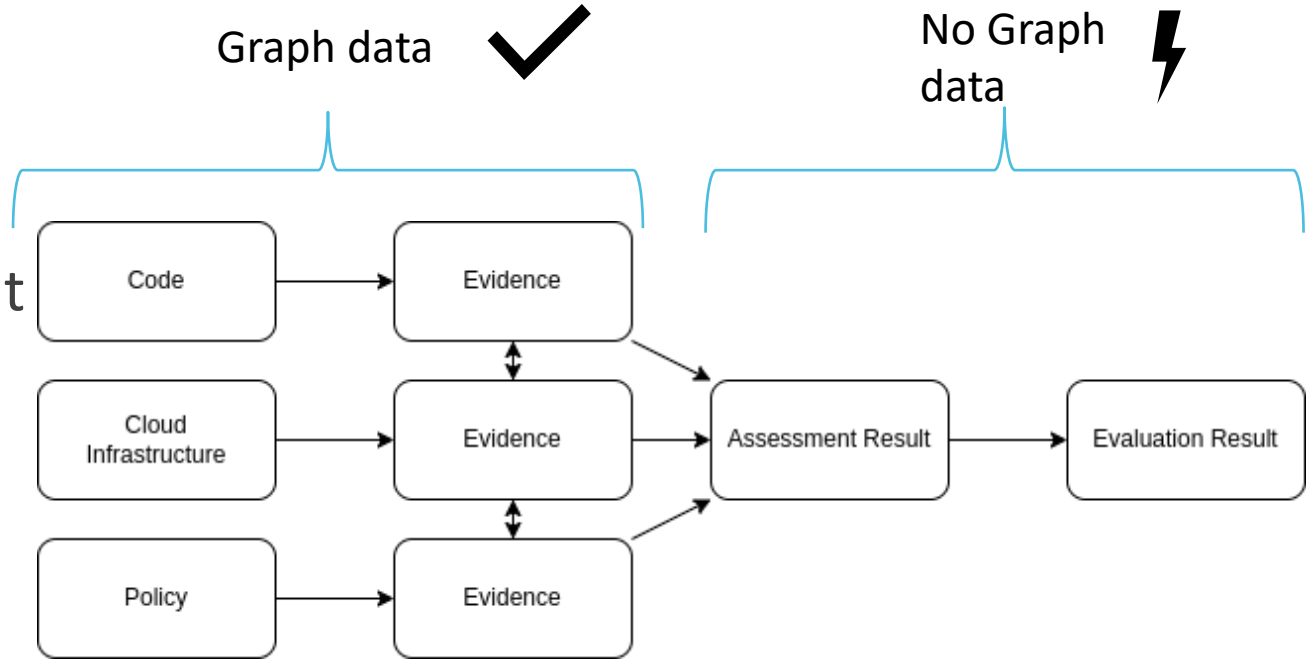


A → B: A pushes data to B
A ⇢ B: B pulls data from A

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



2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping

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

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)

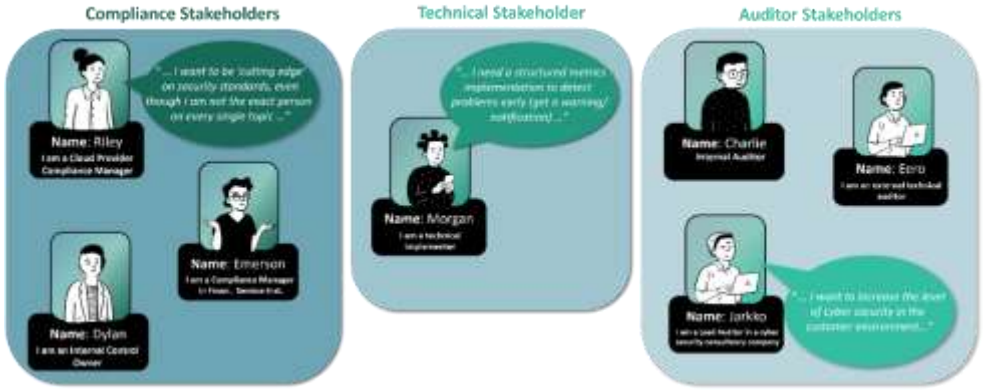
- Provides trustworthiness, fairness and transparency to the evidence and assessment results
- General-purpose semi-public Blockchain infrastructure, which supports services in accordance with European regulations

4 Provide a seamless user experience of continuous auditing for auditors and auditees

EMERALD UI/UX

User interaction concept and conducted studies to show what information each user needs in an audit process

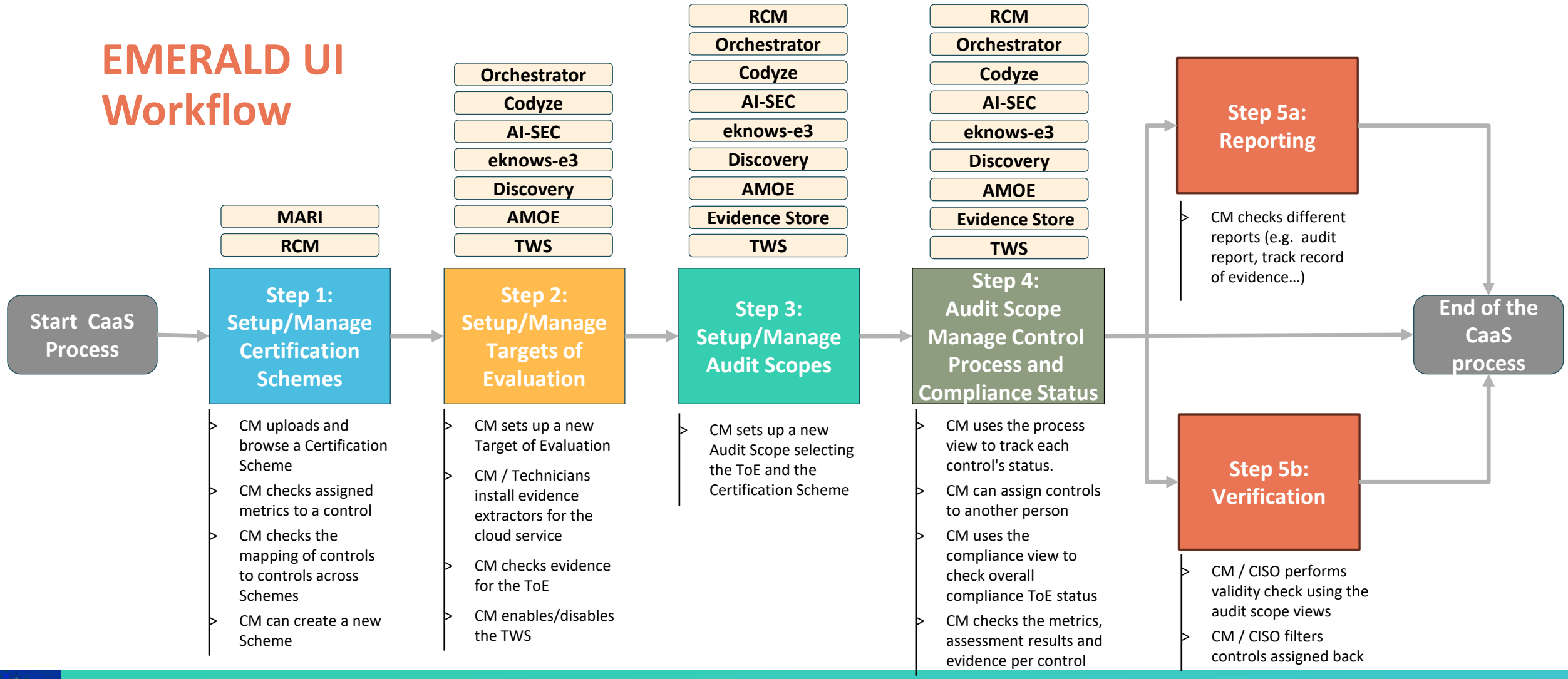
- **User-centered** requirements
- **7 Personas** divided into 3 stakeholder groups
- **Work process modelling**: scenarios and user journeys to define interactions
- **UI/UX design**: Created paper and clickable mock-ups through iterative co-design



4 Provide a seamless user experience of continuous auditing for auditors and auditees

EMERALD

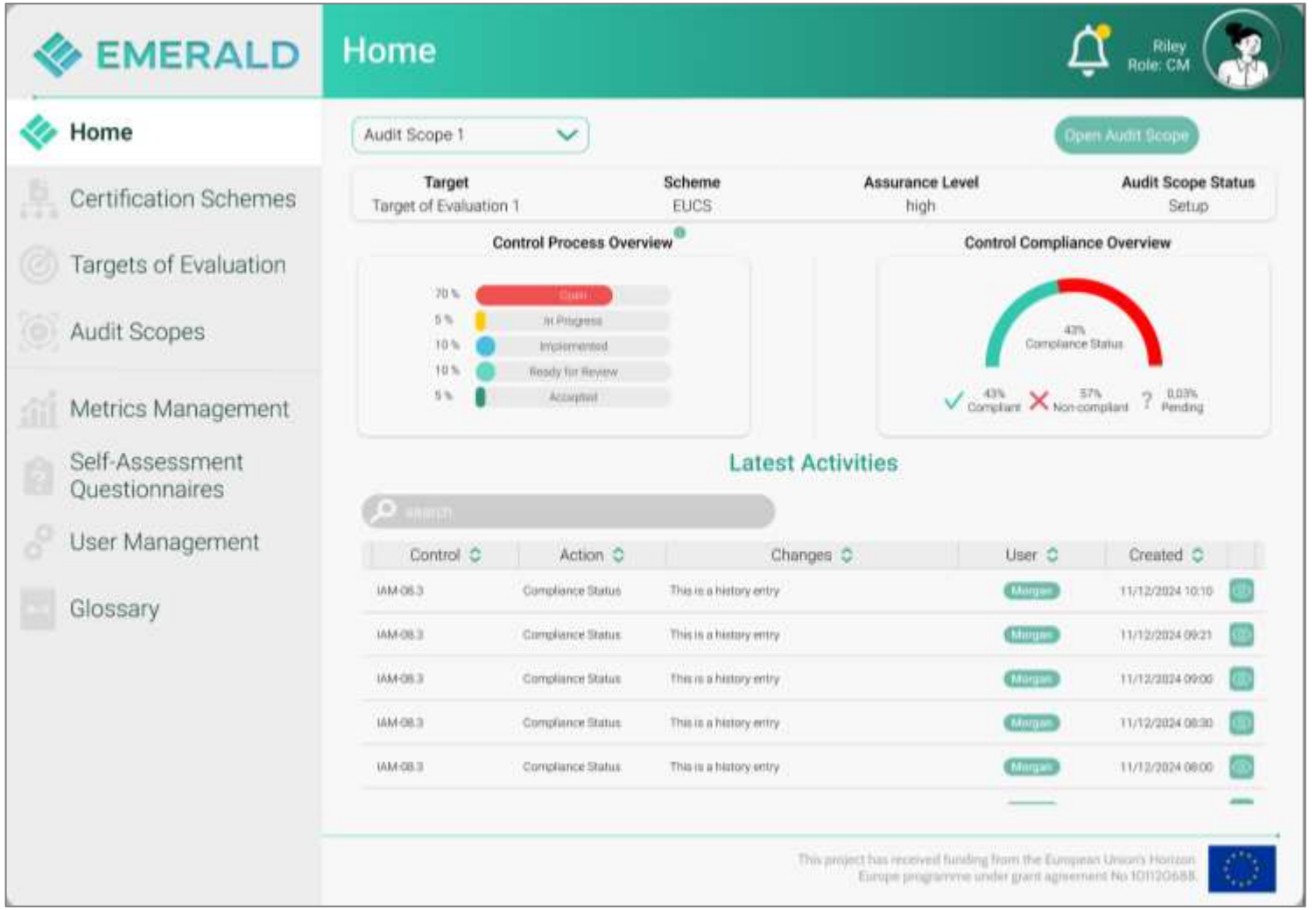
EMERALD UI Workflow



4 Provide a seamless user experience of continuous auditing for auditors and auditees

EMERALD UI implementation

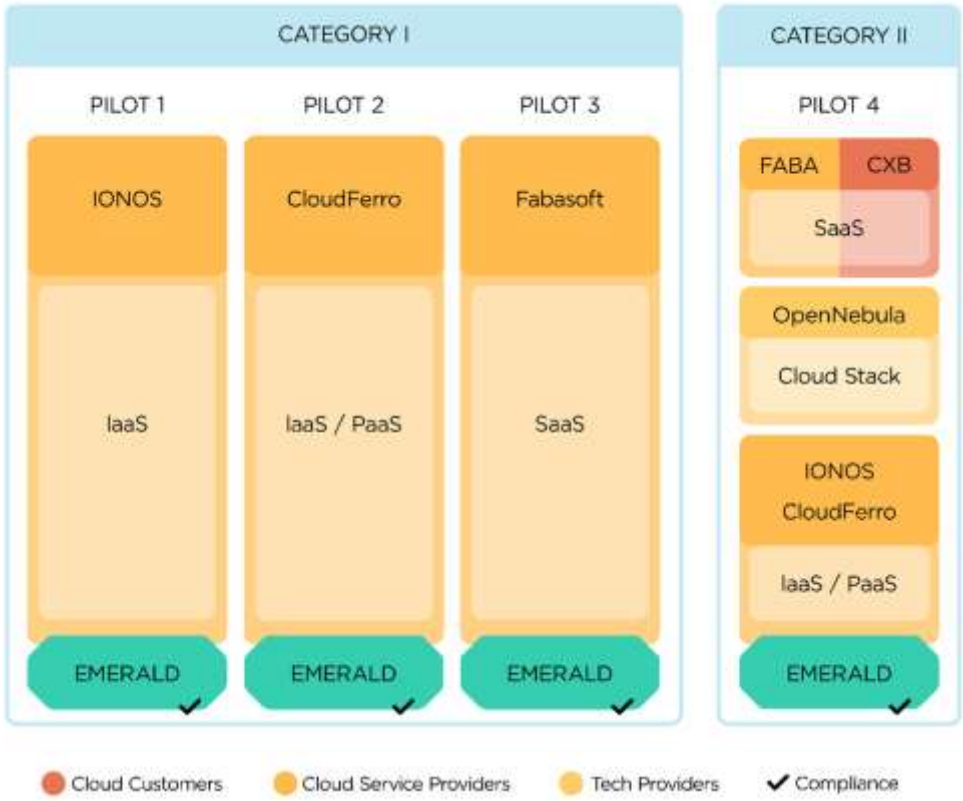
Using NextJS, React and Keycloak



5 Provide experimentation in diverse use cases

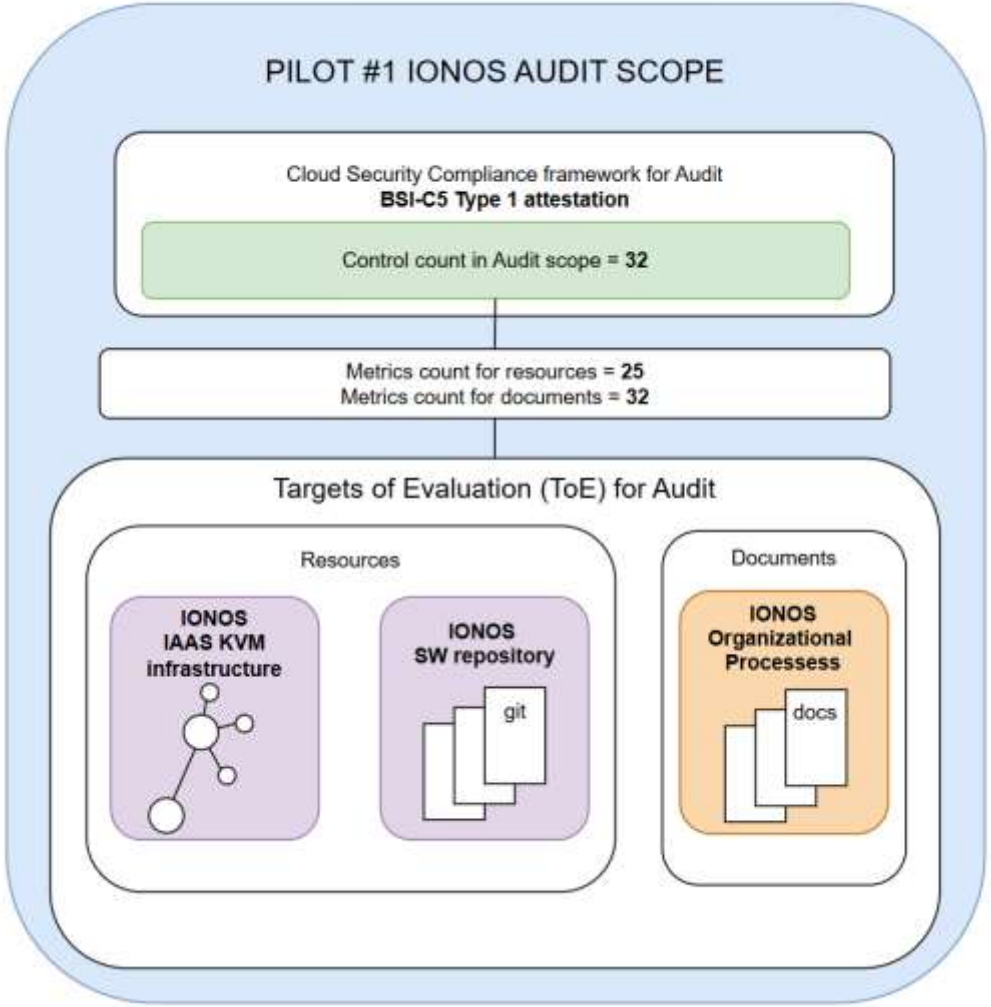
Industrial pilots

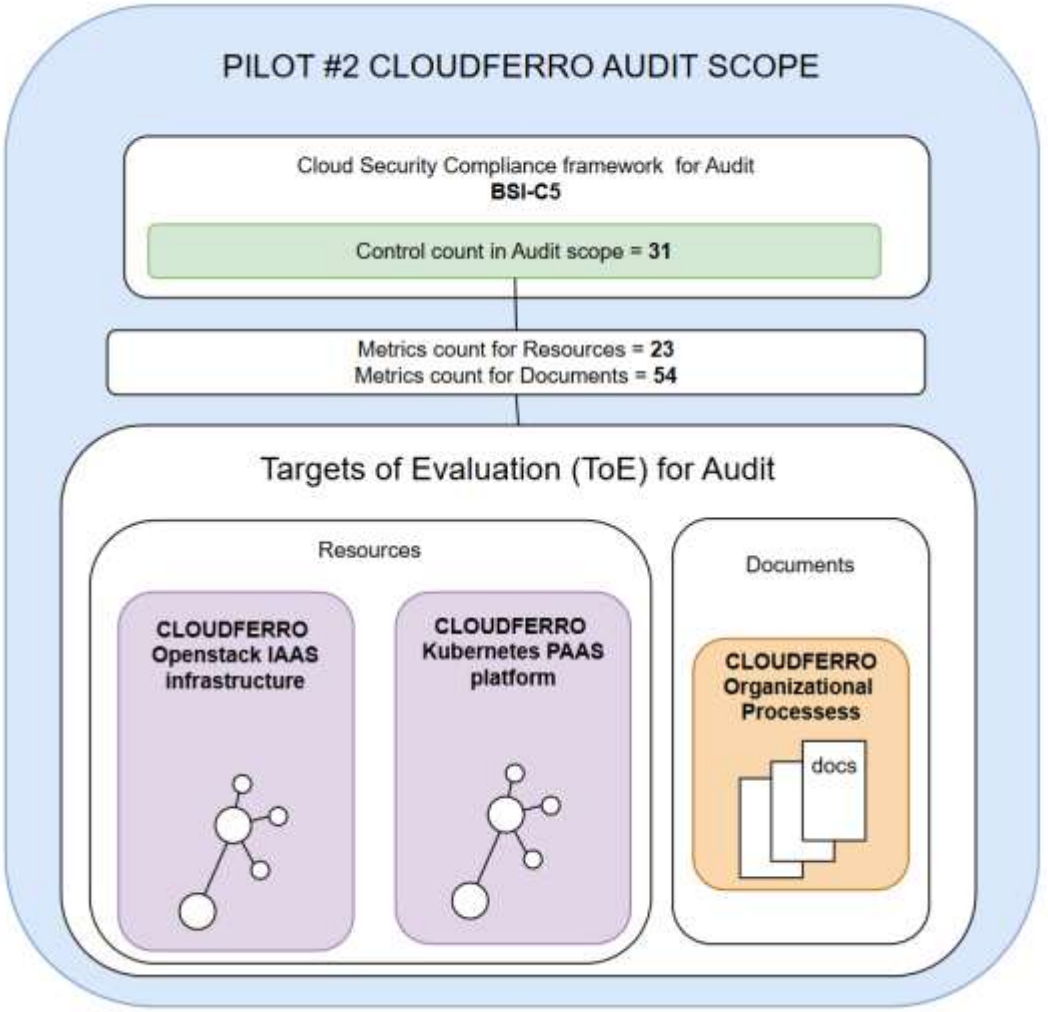
- **Category I:** Certification of public Cloud Services (IaaS, PaaS, SaaS)
- **Category II:** Certification of hybrid cloud-edge environments for the financial sector



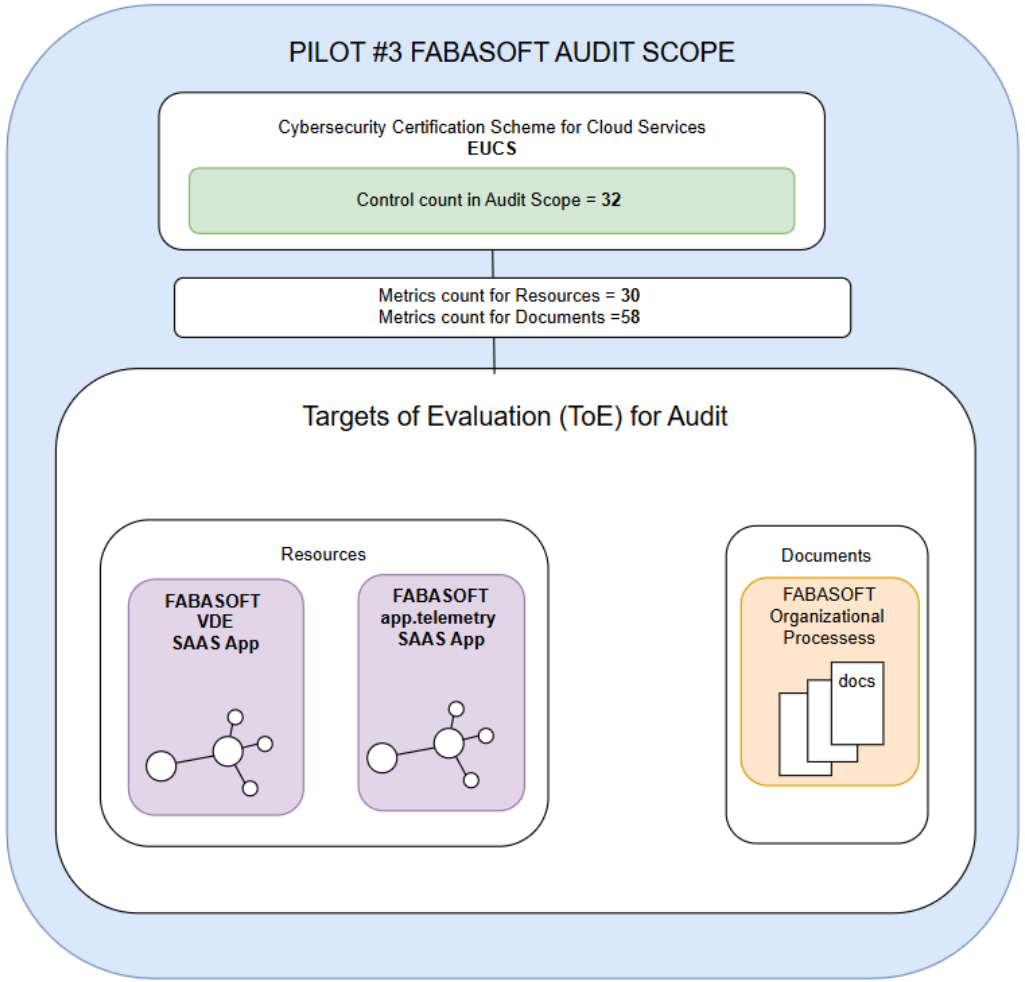
USE CASES AND IMPACT

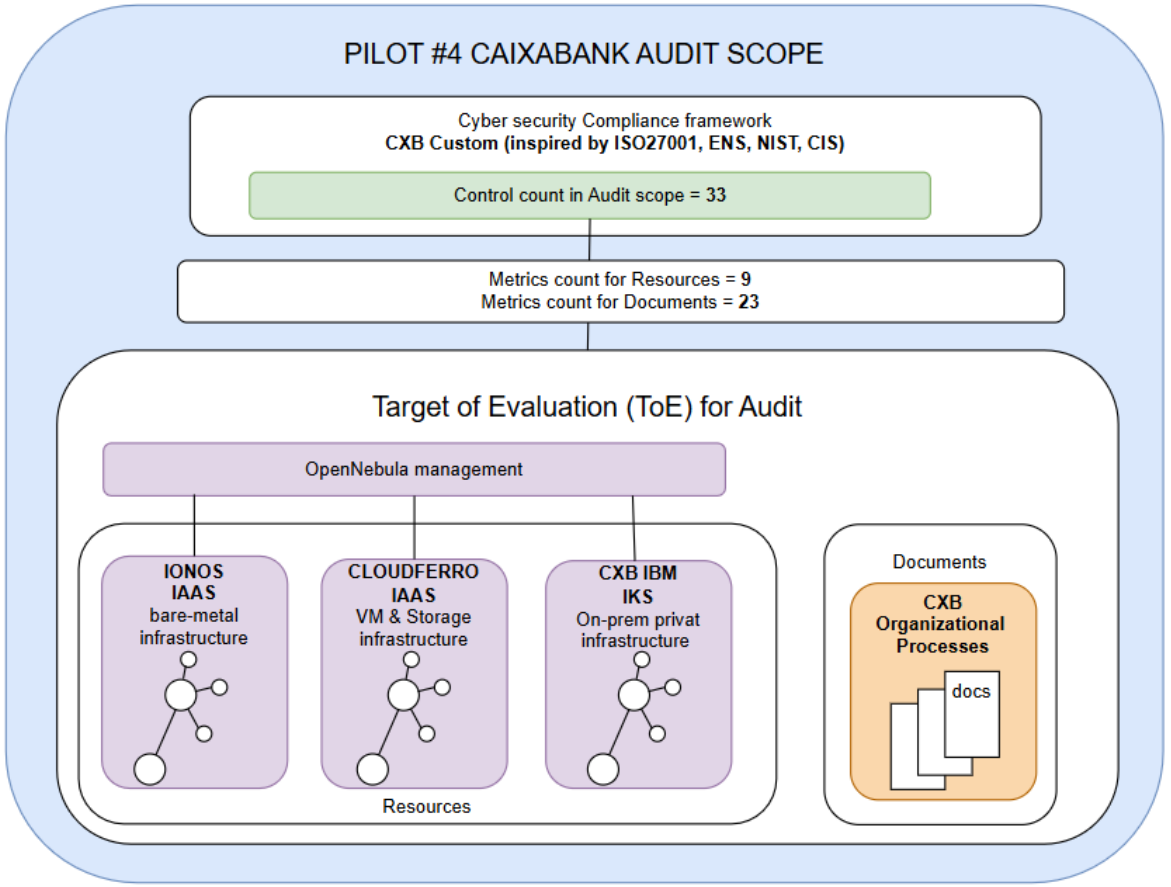
Audit Scope for Pilot 1 and Pilot 2





Audit Scope for Pilot 3 and Pilot 4





In a nutshell

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

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!