

EMERALD

OSCAL in the 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 and OSCAL

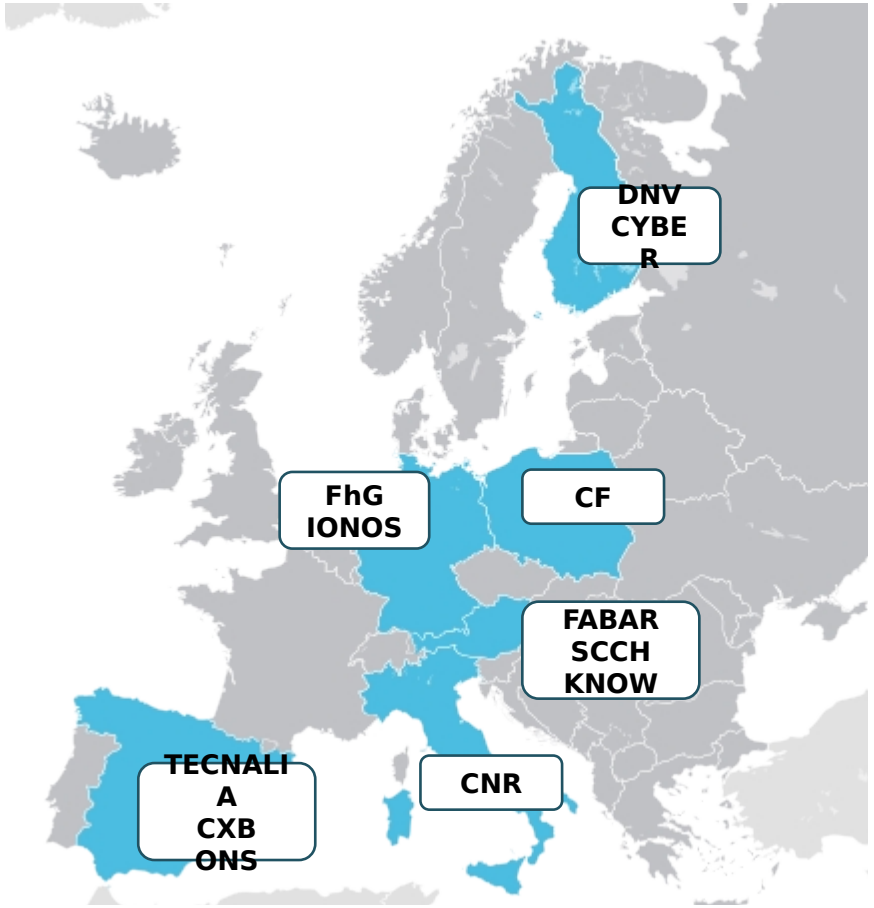
- Starting in the DoA
  - KR7: INTEROP – Interoperable assessment, evidence and catalogue data
    - *Security schemes are prone to change and thus updates would be required. EMERALD aims to mitigate this by incorporating the scheme data in a standardized format such as OSCAL*.
- Collaboration with COBALT in the definition of a common schema for the representation of certification frameworks in OSCAL
- Implementation of an specific module in the RCM to manage import/export of security schemes using OSCAL

Outline

- EMERALD Mission and Objectives
- EMERALD CaaS framework Architecture
- OSCAL in EMERALD
- Demo
- Next steps

EMERALD Innovation Action

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



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 EUROPEAN UNION AGENCY FOR CYBERSECURITY

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.

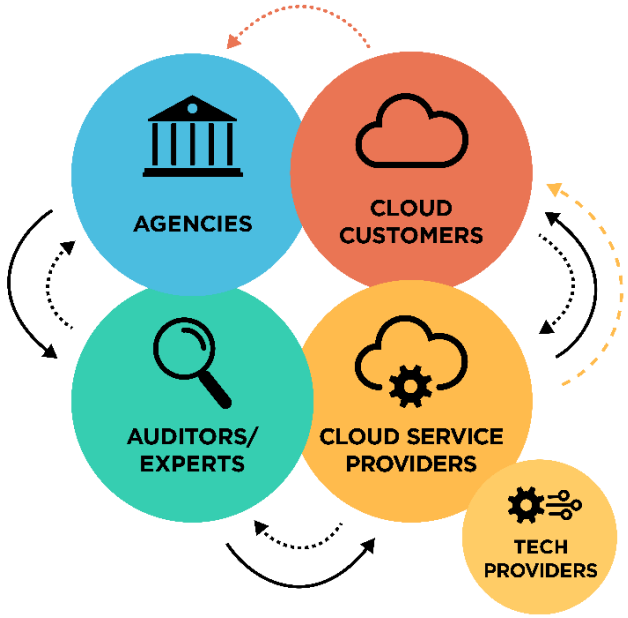
Target users

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**.

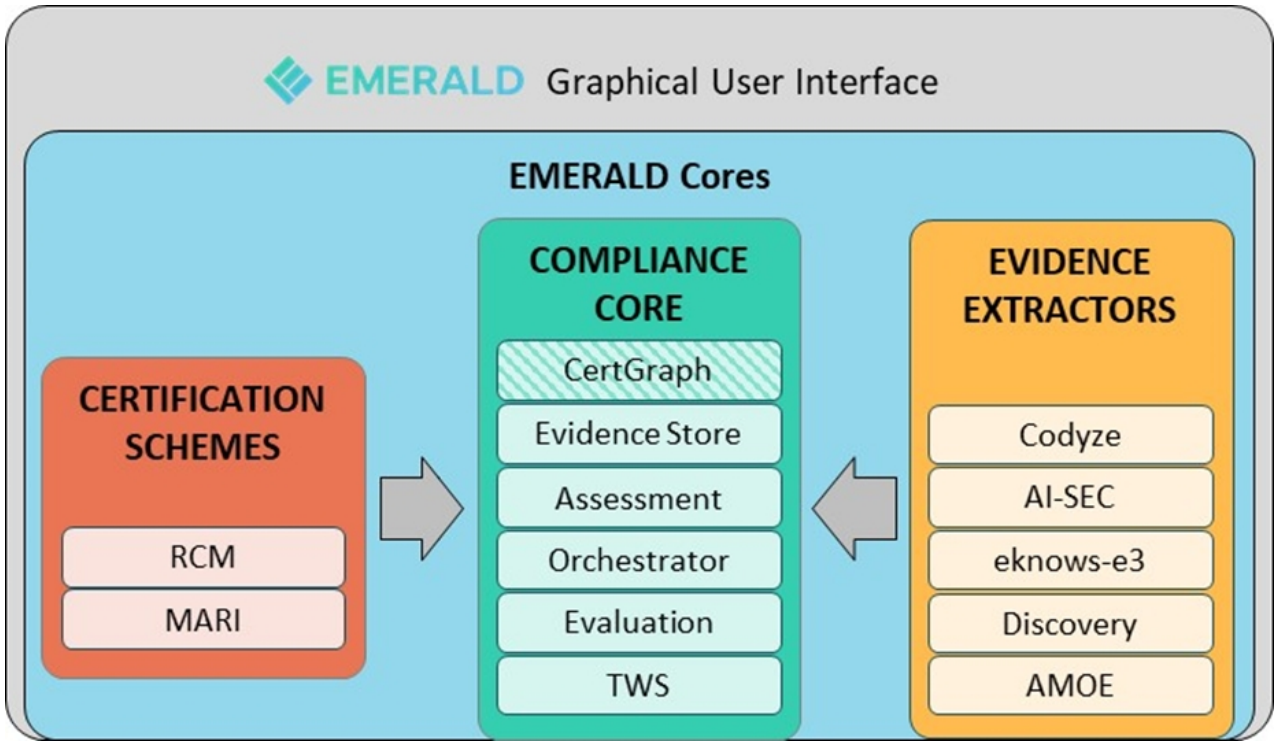
Auditors: EMERALD will offer an **audit assistance framework** to address audits in a uniform manner and reduce complexity by customizing the audit process.

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.



EMERALD CaaS framework Architecture

EMERALD CaaS Building blocks



EMERALD Gitlab Repository

EMERALD GUI: harmonized interface, offering a human centered application

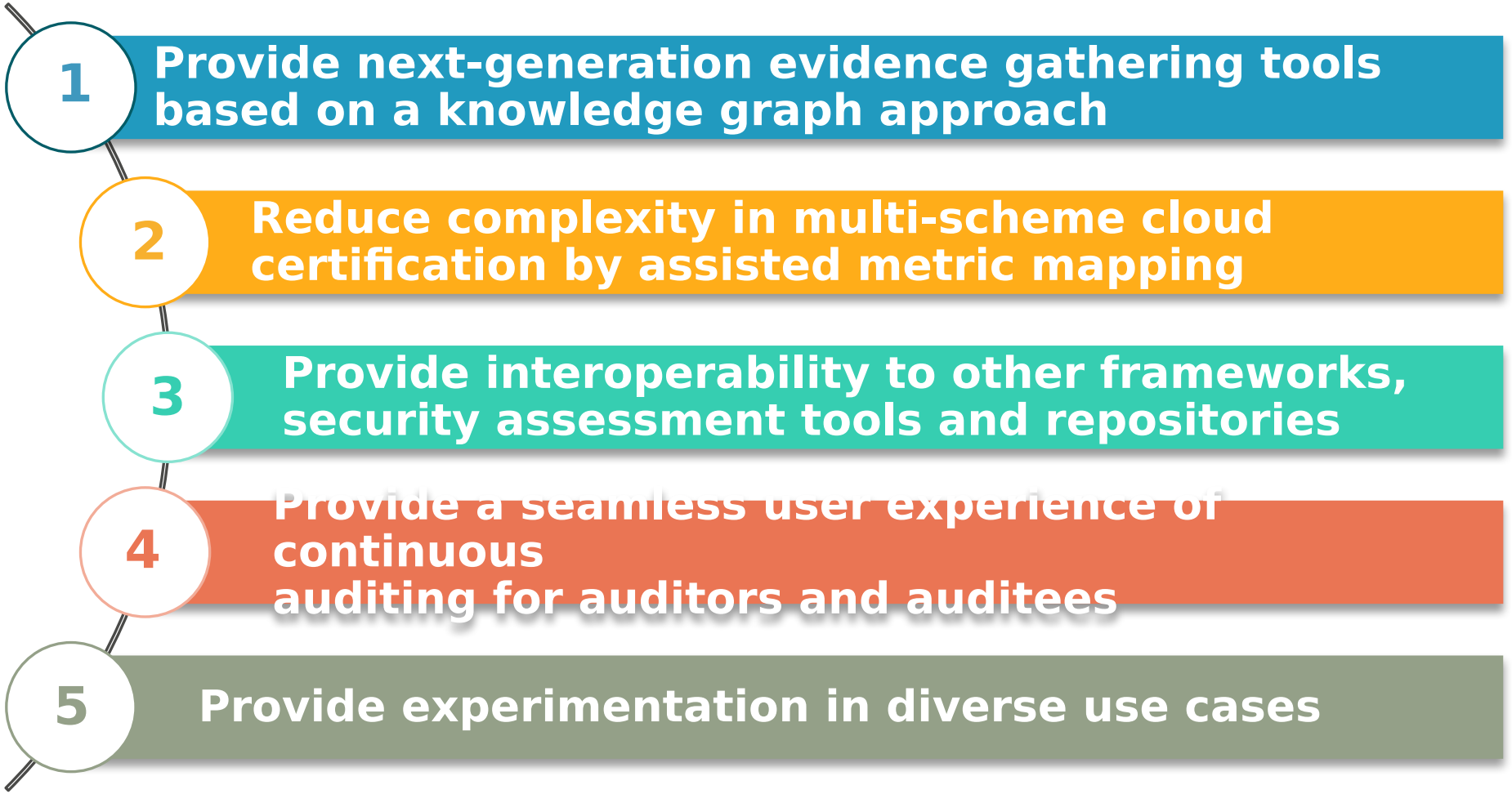
EMERALD CORES: manage heterogeneity and provides abstraction

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

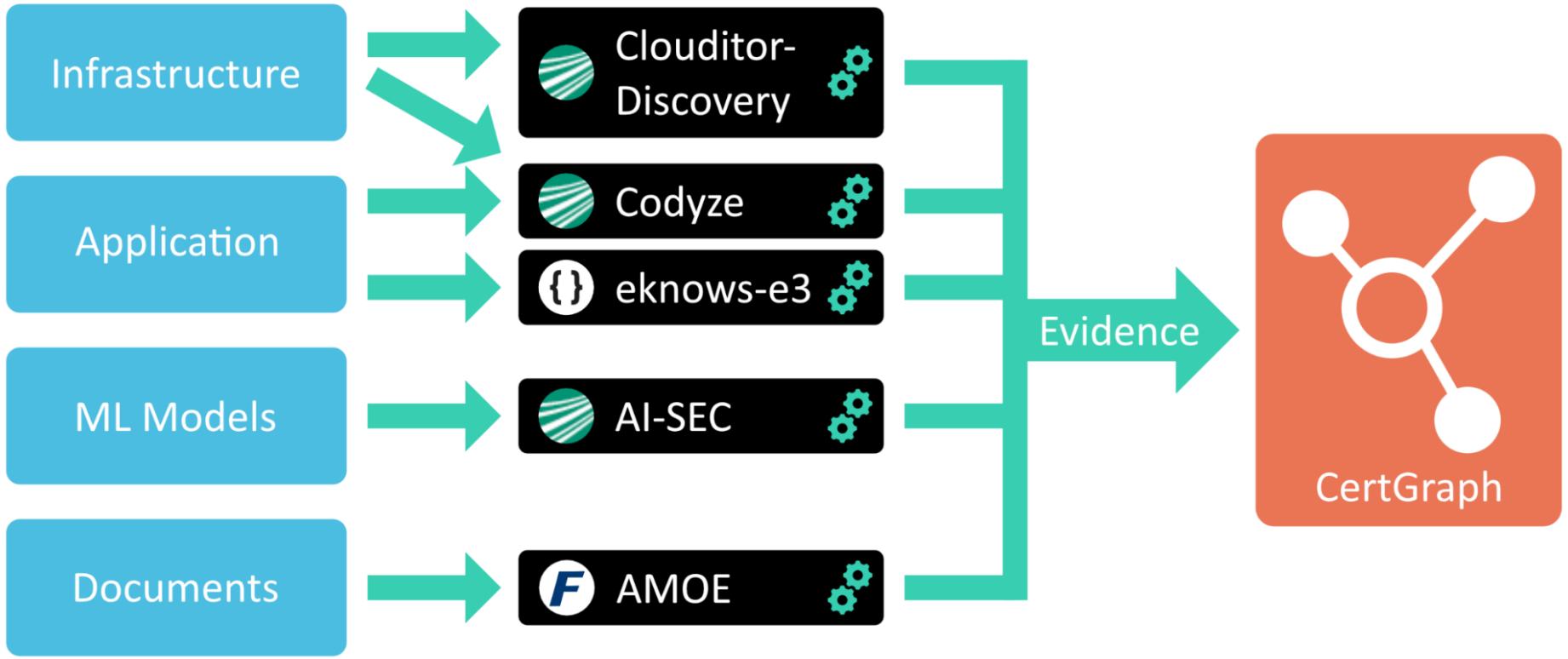
EVIDENCE EXTRACTORS: Evidences extraction from different sources

EMERALD CaaS Goals



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

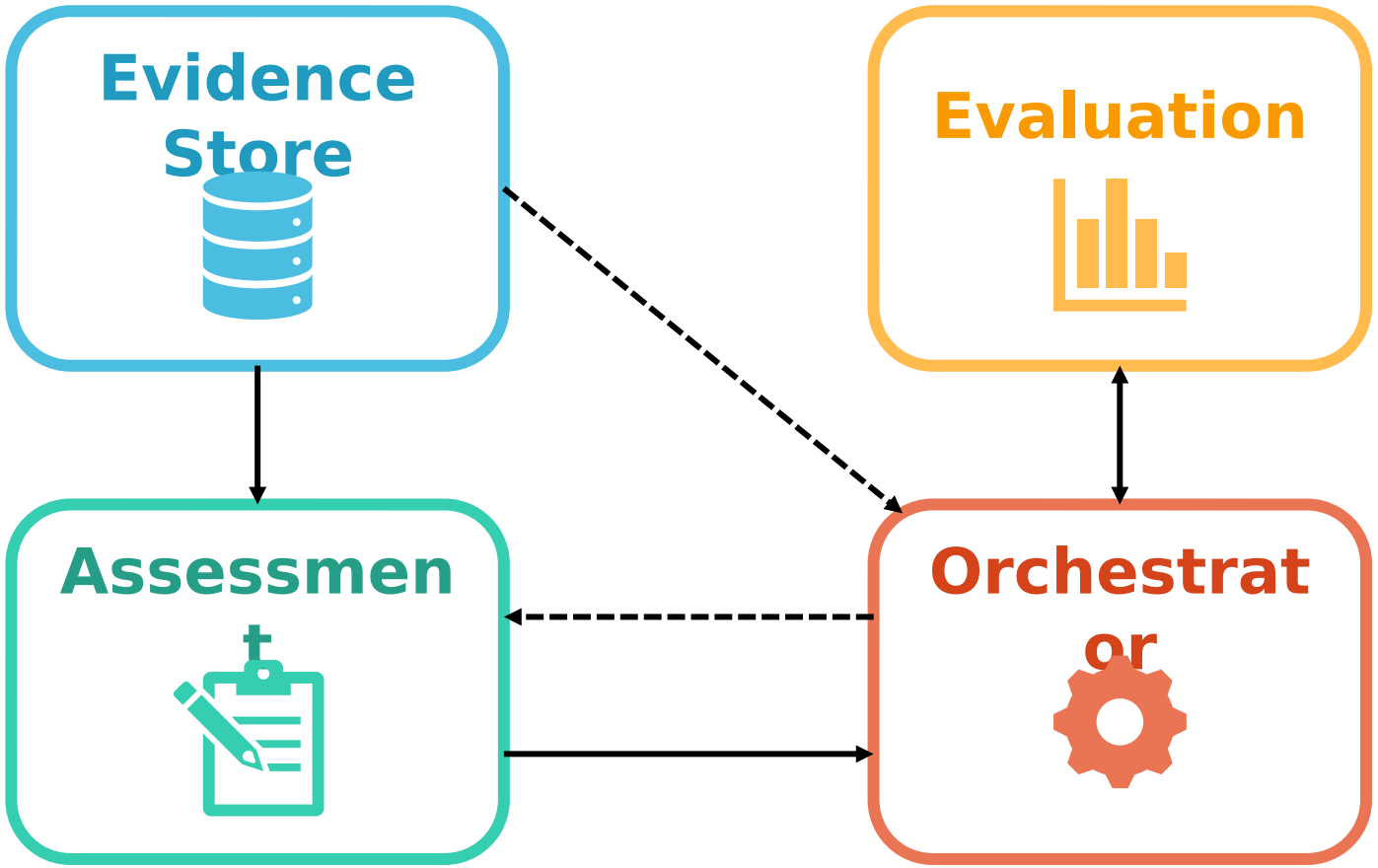
EMERALD



1 **Evidence Extraction**

2 **Unified graph model**

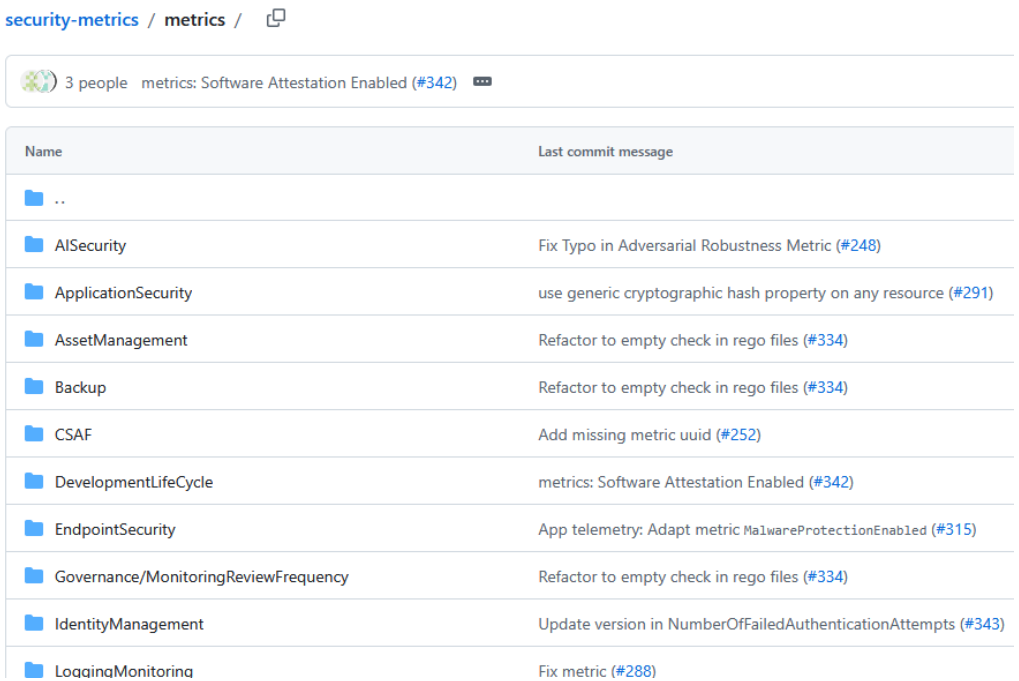
2 Reduce complexity in multi-scheme cloud certification by assisted metric mapping



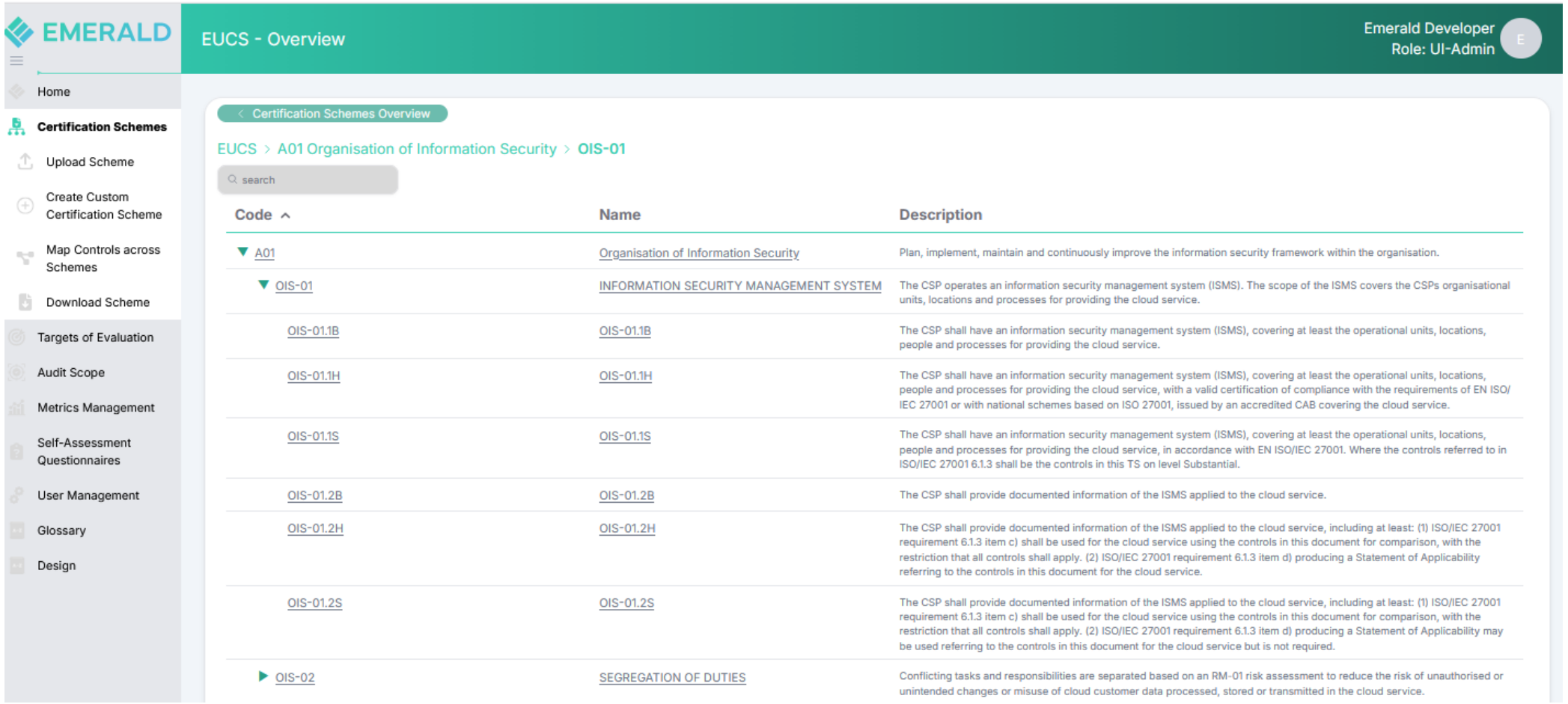
A → B: A pushes data to B
A ⇢ B: B pulls data from A

Repository of Controls & Metrics (RCM)

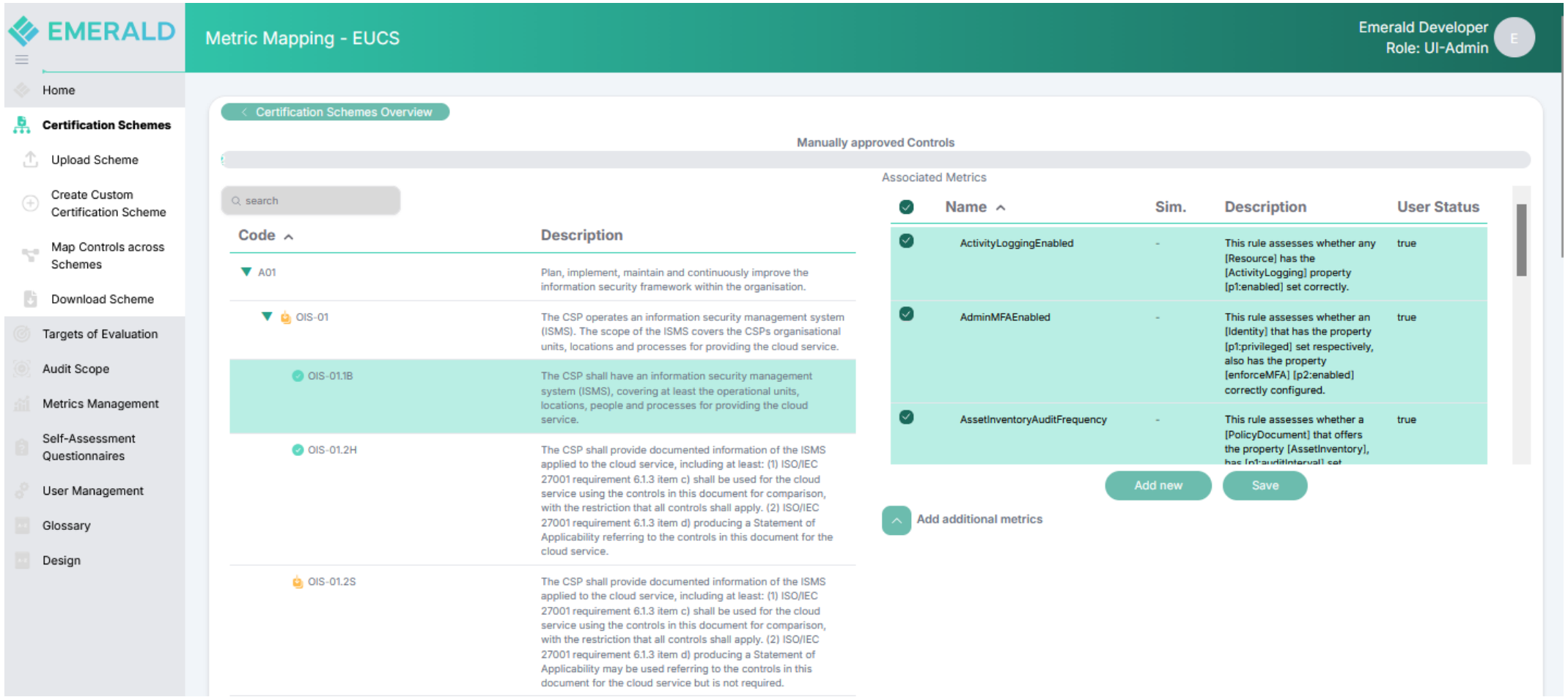
- Multi-schema support: controls from EUCS, BSI-C5, BSI-AIC4, ENS, NIST, CIS
- Reuse of controls through mapping
- Support of personalized schemas
- Extensible and interoperable: import/export mechanisms (OSCAL)
- Metric source: Security Metrics Repos



3 Provide interoperability to other frameworks, security assessment tools and repositories

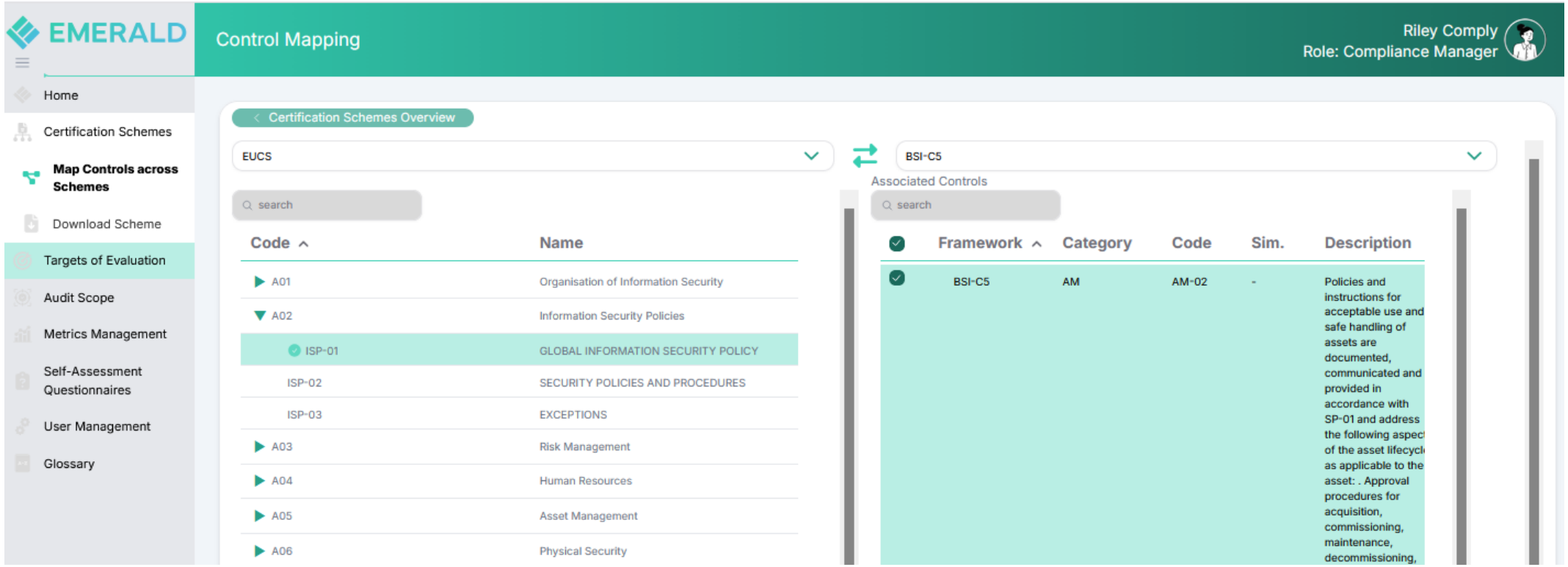


3 Provide interoperability to other frameworks, security assessment tools and repositories



3 Provide interoperability to other frameworks, security assessment tools and repositories

EMERALD

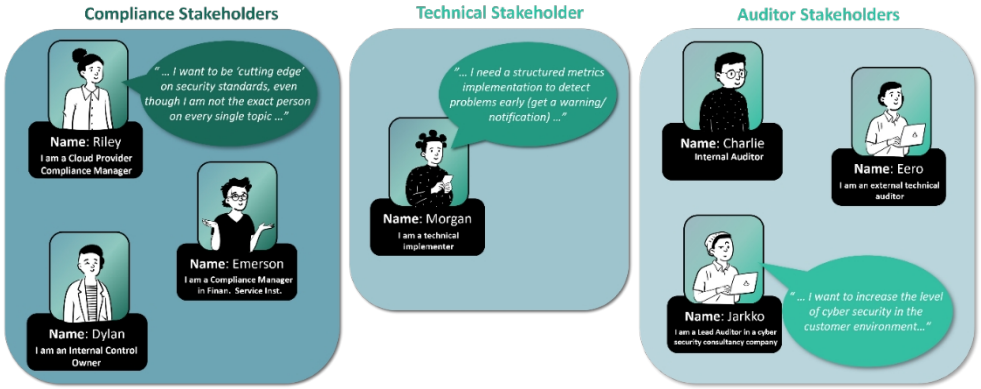


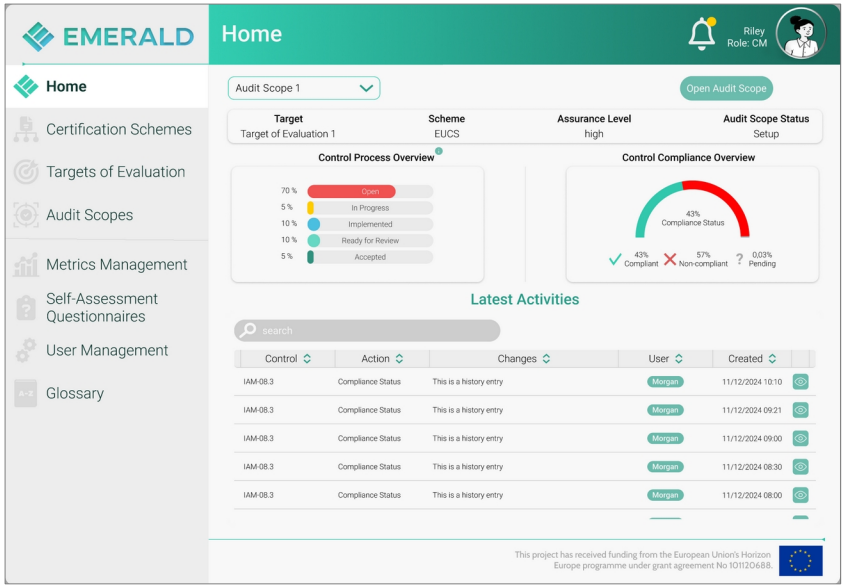
4 Provide a seamless user experience of continuous auditing for auditors and auditees

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

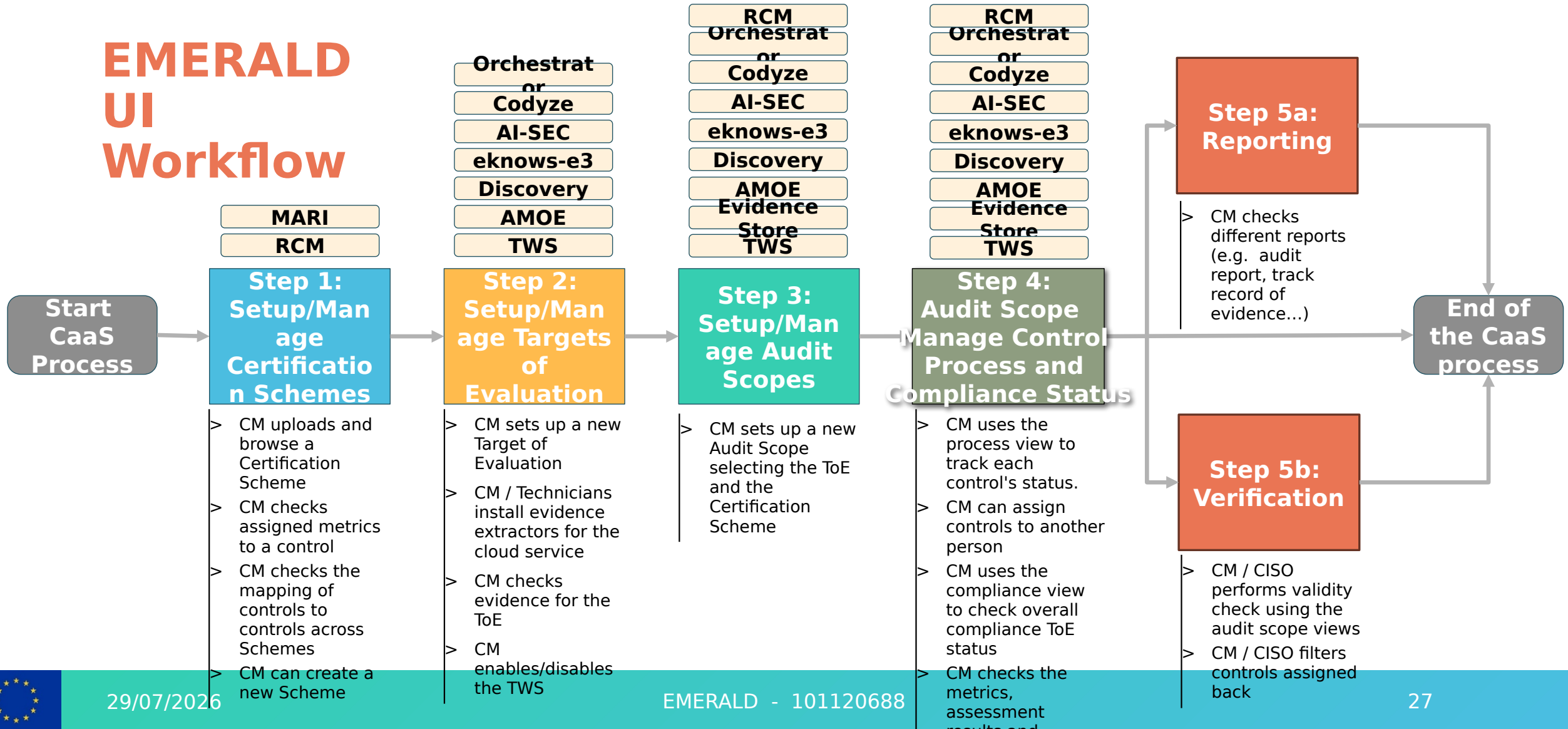




4 Provide a seamless user experience of continuous auditing for auditors and auditees

EMERALD

EMERALD UI Workflow



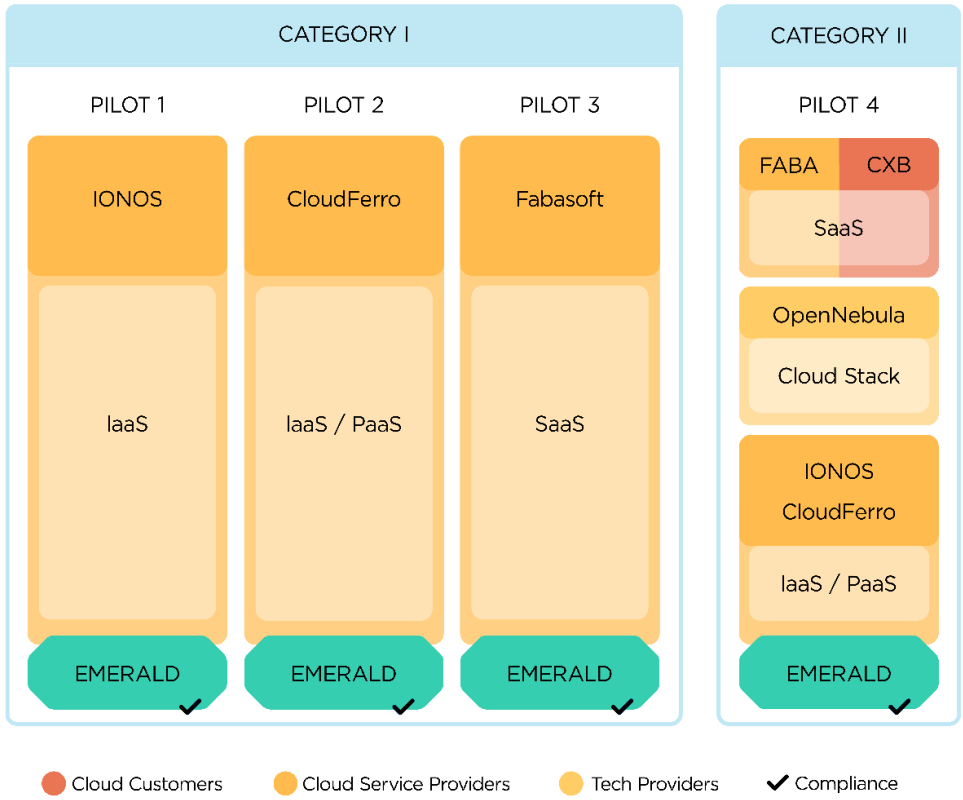
5 Provide experimentation in diverse use cases

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 Open Nebula CaixaBank



OSCAL in EMERALD

OSCAL in EMERALD

Objective:

- Provide some interoperability across tools and organizations

How:

- Import/export OSCAL schemes from/to EMERALD Repository (RCM)

Steps:

1. Define a **“generic” Framework** OSCAL (json) template
2. **Export** from RCM DB to OSCAL template
3. [**Import** from any template-compliant OSCAL framework to RCM DB]

OSCAL template overview

OSCAL

Controls Layer\Catalog Model

- Groups
- Controls
- Parts
- Properties
- Prose

EUCS

EUCS Framework

- Domain
- Category
- Objective
- Control ID
- Control
- Control Objective
- Requirement ID
- Requirement

OSCAL template (I)

```
{
   "catalog":
   {
      "uuid": "12152641-cd61-4bb8-ab67-0e9...",
           "metadata":
      {
           "title": "EUCS",
           "published": "2026-01-11",
           "last-modified": "2026-01-11",
           "version": "1.0",
           "oscal-version":
"1.1.2", ...
      },
   ...
```

The **Framework** is implemented within a OSCAL Catalog element, identified by an **UUID** and defined by other applicable **metadata**

Framework

OSCAL template (II)

```
"controls": [
{
   "id": "eucs-A03.RM-01",
   "class": "eucs",
   "title": "RM-01 RISK MANAGEMENT POLICY",
   "props": [
      {
         "name": "label",
         "value": "RM-01"
      }
   ],
...
```

EUCS' **Domains** and **Categories** are created as elements of the OSCAL "groups" array, with the name in the attribute "title".

Objective is represented using the "parts" element with "name" and "prose".

EUCS **Controls** are gathered in the "controls" array, represented by an "id" and a "title" in OSCAL.

- Domain
- Category
- Objective
- Control ID
- Control

OSCAL template (III)

```
"parts":[
  {
  "id": "eucs-A03.RM-01_obj_1",
  "name": "statement",
  "props":[...],
  "prose": "Risk management policies and procedures are documented and communicated to stakeholders."
  },
  {
  "id": "eucs-A03.RM-01_req",
  "name": "statement", "props":[ ...
     {
     "name": "alt-identifier",
     "value": "Requirements"
     }
  ],
  "parts":[
     {
     "id": "eucs-A03.RM-01_req.1B",
     "name": "item",
     "class": "basic",
     "props":
        {
        "name": "alt-identifier",
        "value": "RM-01.1B",
        "class": "basic"
        },
        "prose": "The CSP shall define policies and procedures for the cloud service
     in accordance with ISP-02 and OIS-01.1B for the following aspects... },
...
```

The Control **Objective** is added within “parts” as “prose”.

EUCS **Requirement set** is implemented as a nested “parts” within the Control, with the Description as “prose” and the ID and Assurance Level specified within “props”.

- Control Objective
- Requirement ID
- Requirement

OSCAL template summary

Mapping EUCS to OSCAL Catalog model		
OSCAL Catalog Model	EUCS element	Example
Groups/ID	Domain	A7
Groups/title	Category	A7 Operational Security
Groups/parts/prose(objective)	Objective	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Groups/Controls/properties/value(label)	Control ID	OPS-02
Groups/Controls/title	Control	CAPACITY MANAGEMENT - MONITORING
Groups/Controls/parts/prose/(control-objective)	Control Objective	The capacities of critical resources such as personnel and IT resources are monitored.
Groups/Controls/parts/parts/properties/value(label)	Requirement ID	OPS-02.3
Groups/Controls/parts/parts/prose(item)	Requirement	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1

DEMO

EMERALD-OSCAL demo

1. **Select a scheme** from the EMERALD list (EUCS)
2. **Export** the framework to a file
3. **Review** the file structure/content
4. **Import** the same file calling manually the RCM API
5. **Check the new scheme** in EMERALD GUI

OUTSIDE EMERALD *

(*) Import still to be integrated in the EMERALD GUI

www.emerald-he.eu

@emerald-he-project

emerald-he-project



Scan