EMERALD

Cybersecurity certification for the Computing Continuum: Future Challenges and opportunities

UM- Master in CyberSecurity

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

About

EMERALD

TECNALIA research center

EU Project Director

Senior Researcher: Cloud Computing PhD

ECCO (European Cyber Security Community) Roadmapping WG

E3C (European Cluster for Cybersecurity Certification)

DOME (Distributed Open Marketplace for Europe)

Juncal Alonso

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Outline for the session

EMERALD

	Ice breaking session : General topics and concepts	5 min
	Cybersecurity certification for the Computing Continuum. Future Challenges and opportunities	10 min
	EMERALD: Towards Automatized Compliance as a Service for the Computing Continuum	45 min
	Open discussion and questions	30 min

Outline for the session

EMERALD

Ice breaking session : General topics and concepts	5 min
Cybersecurity certification for the Computing Continuum Future Challenges and opportunities	10 min
EMERALD: Towards Automatized Compliance as a Service for the Computing Continuum	45 min
Open discussion and questions	30 min

Context and motivation

EMERALD

EU Digital sovereignty towards competitive and heterogeneous Cloud Continuum sector

Tsunami of Regulations (EUCS, AI Act, Data Act, CADA, CRA, NIS2…)

SMEs and distributed nature of European Cloud Ecosystem

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

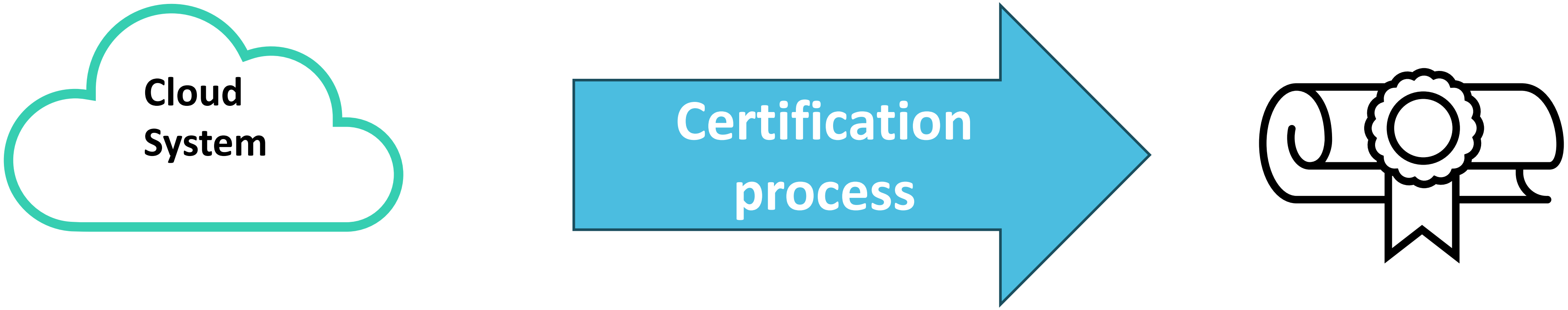
Uncertainty on how to technically achieve EUCS level high

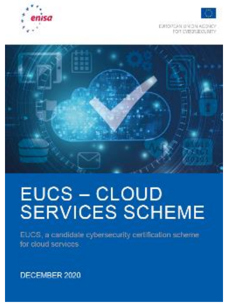
Geopolitical and Technical challenges

*Images source: Generated by COPILOT

** Image source : ENISA

Context and motivation




enisa

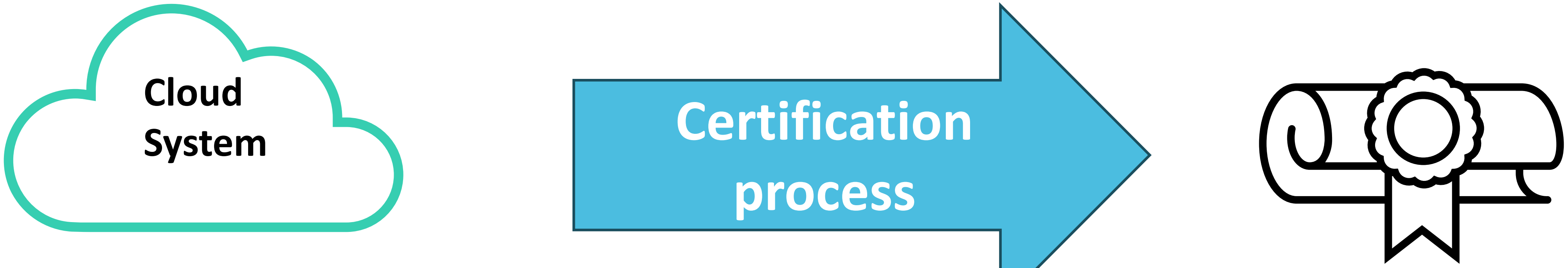
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

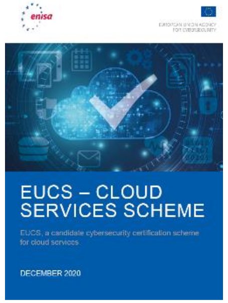
DECEMBER 2020

Context and motivation



Infrastructure
Application
ML (AI) models
Organizational processes

Tedious
Time Consuming
Costly
….



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

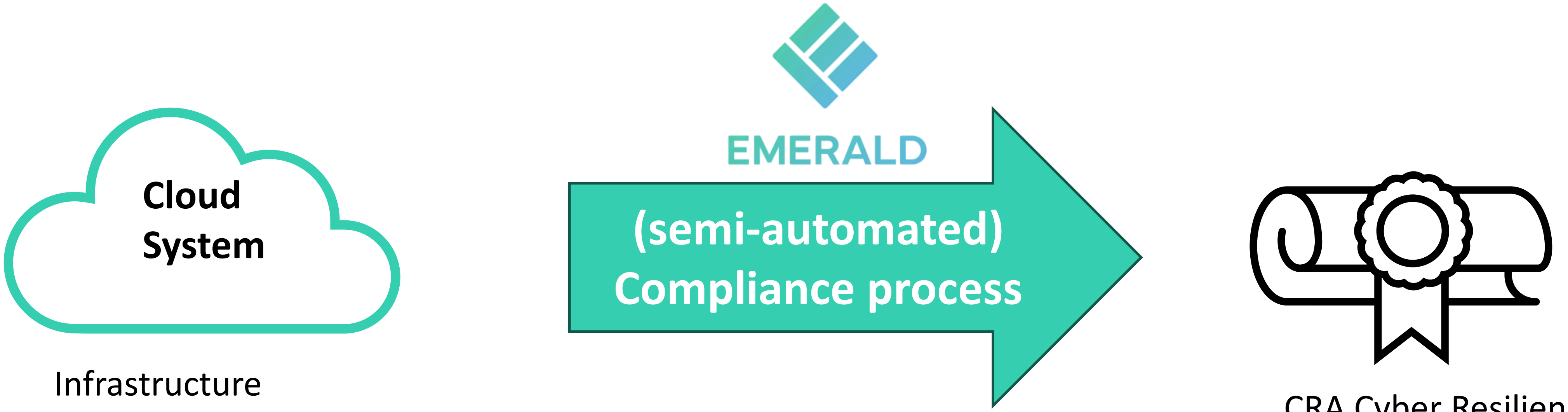
EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

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

Context and motivation



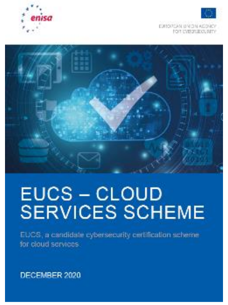
Cloud System

EMERALD

(semi-automated) Compliance process

Infrastructure
Application
ML (AI) models
Organizational processes

Tedious
Time Consuming
Costly
….



EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

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

Outline for the session

EMERALD

Ice breaking session : General topics and concepts	5 min
Cybersecurity certification for the Computing Continuum Future Challenges and opportunities	10 min
EMERALD: Towards Automatized Compliance as a Service for the Computing Continuum	45 min
Open discussion and questions	30 min

EMERALD Innovation Action

EMERALD

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

tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fraunhofer AISEC

Fabasoft

Consiglio Nazionale delle Ricerche

scch { } software competence center hagenberg

KNOW Center

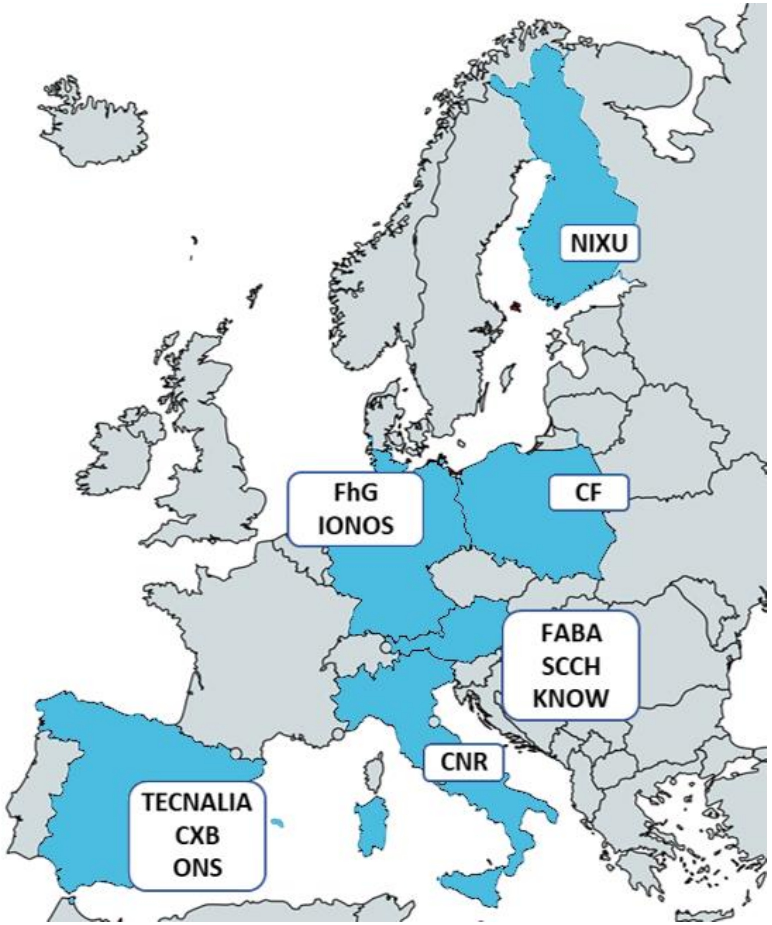
CaixaBank

IONOS

CloudFerro

Open Nebula

DNV CYBER



EMERALD Mission

- 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 **focus on evidence management components** for the **continuous compliance approach.**
- EMERALD **provides 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•

Driving the CaaS Vision: EMERALD’s Core Mission

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 metric mapping**.

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.

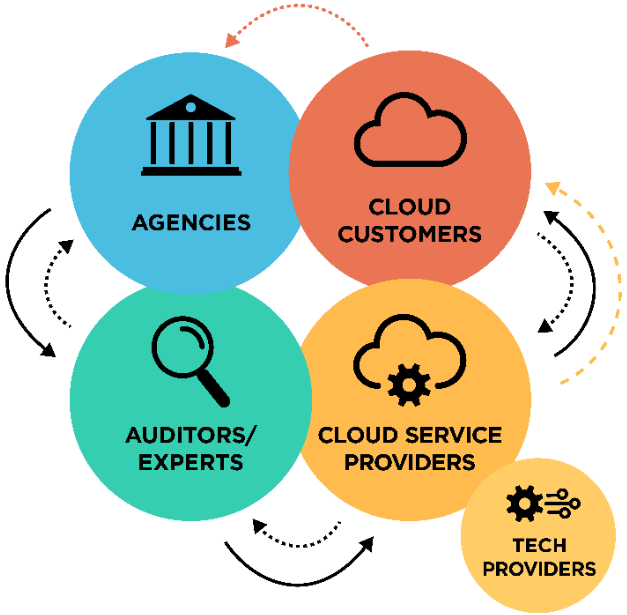
Target users

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.



Addressing the challenges in cloud security certification with EMERALD

EMERALD

Next-generation evidence gathering tools based on a knowledge graph approach

- Knowledge extraction on various layers of the cloud service (infrastructure, code, policy documents) and prepare suitable evidence based on them.
- A graph-based structure to consolidate all necessary information of the service and to make it easily query-able, linking heterogeneous information extracted from different evidence sources.

Reduce complexity in multi-scheme Cloud certifications by assisted metric mapping

- An intelligent system to select an optimized set of metrics that can be measured to demonstrate compliance to the selected certification scheme.
- A tool to assess chosen metrics based on information stored in the certification graph and to evaluate the final certificate decision.
- A proof of concept (PoC) on how to scale the CaaS approach to cloud-based AI systems.

Addressing the challenges in cloud security certification with EMERALD

Seamless user experience of continuos auditing for auditors and auditees

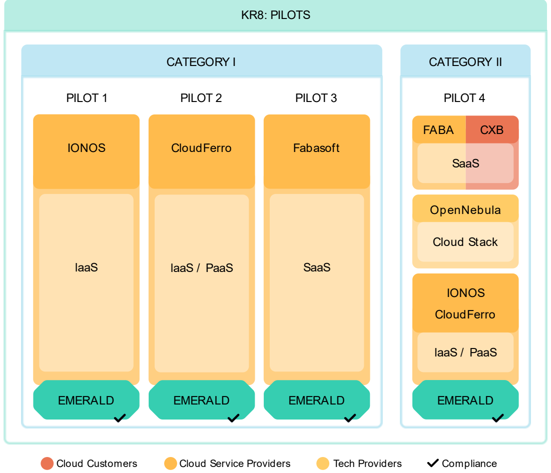
- User interaction concept and conducted studies to show what information each user needs in an audit process

Increased interoperability between frameworks, security assessment tools and repositories

- Interoperability layer among the trustworthy systems, assessment results and catalogue data. Standardized formats such as OSCAL (Open Security Controls Assessment Language) will be used to mitigate the impact of changes in the security schemes.

Experimentation in diverse use cases

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


KR8: PILOTS

CATEGORY I

PILOT 1: IONOS, IaaS, EMERALD ✓

PILOT 2: CloudFerro, IaaS / PaaS, EMERALD ✓

PILOT 3: Fabasoft, SaaS, EMERALD ✓

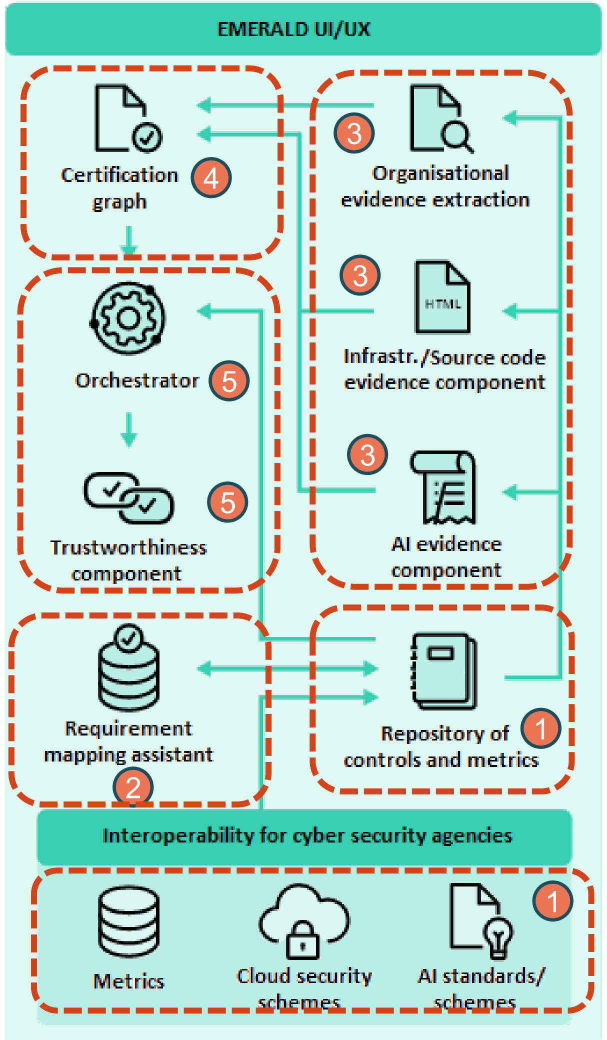
CATEGORY II

PILOT 4: FABA, CXB, SaaS; OpenNebula, Cloud Stack; IONOS, CloudFerro, IaaS / PaaS; EMERALD ✓

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

Approach

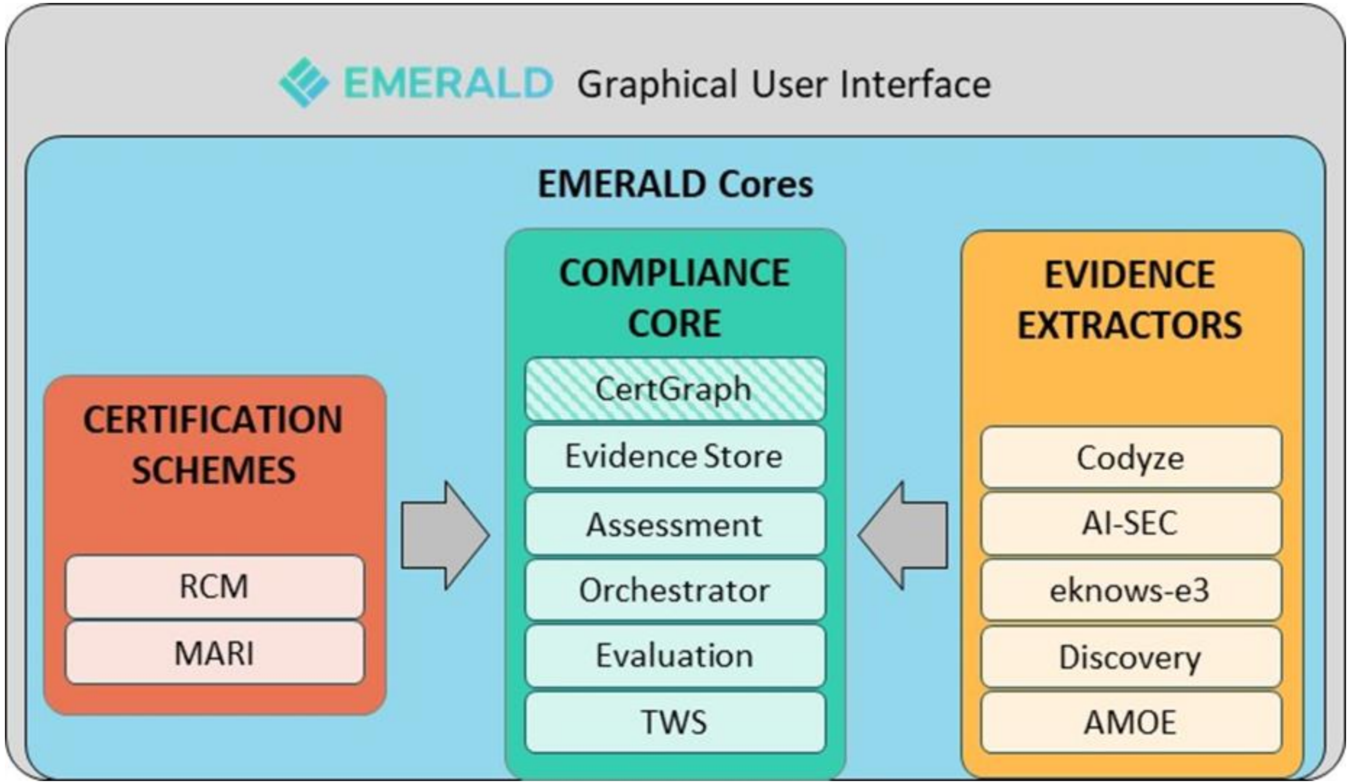
1. Different **controls** from one or more **certification schemes are selected**, which are a comprehensive set of rules, technical requirements, standards and procedures with which to demonstrate compliance.
2. An intelligent system selects an **optimized set of metrics that can be measured** to demonstrate 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 UI/UX
Certification graph
4
3
Organisational evidence extraction
Orchestrator
5
3
HTML
Infrastr./Source code evidence component
3
Trustworthiness component
5
AI evidence component
Requirement mapping assistant
2
Repository of controls and metrics
1
Interoperability for cyber security agencies
Metrics
Cloud security schemes
AI standards/ schemes
1

EMERALD CaaS Building blocks

EMERALD



EMERALD GUI: harmonized interface, offering a human centered application

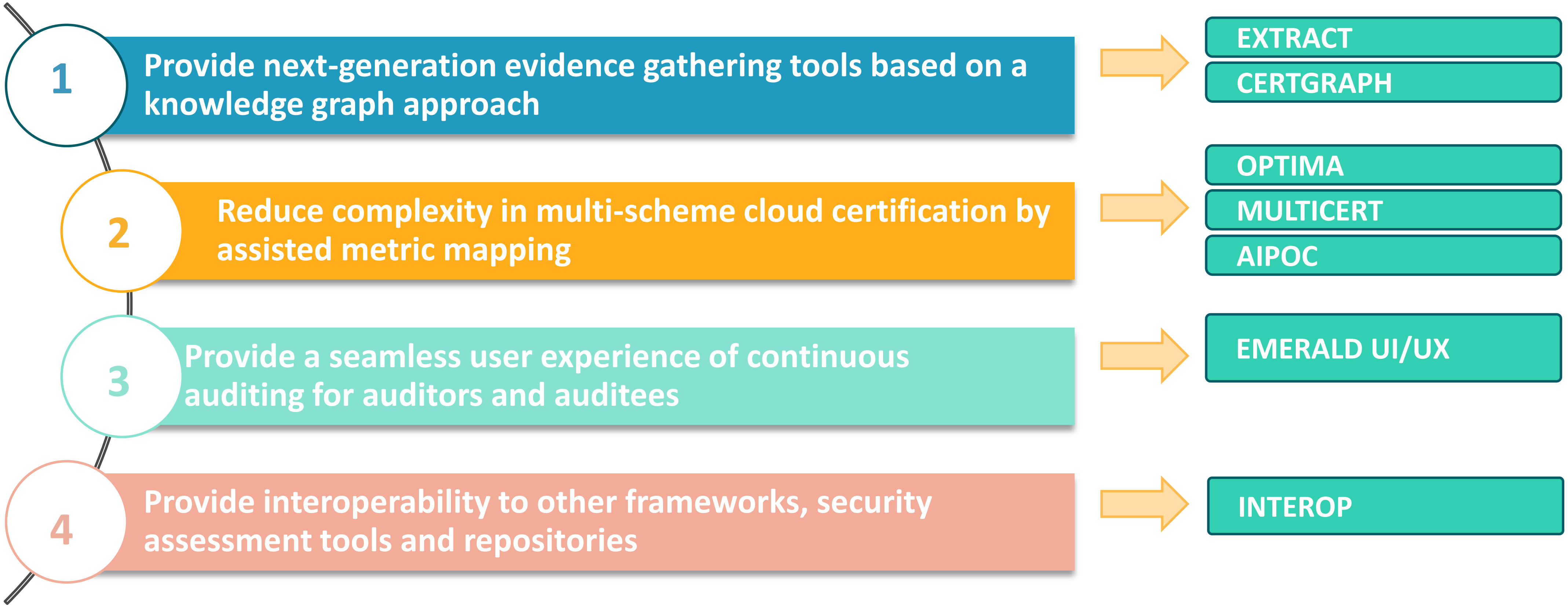
EMERALD CORES: manage heterogeneity and provides abstraction

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 Objectives



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

EXTRACT

CERTGRAPH

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

OPTIMA

MULTICERT

AIPOC

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

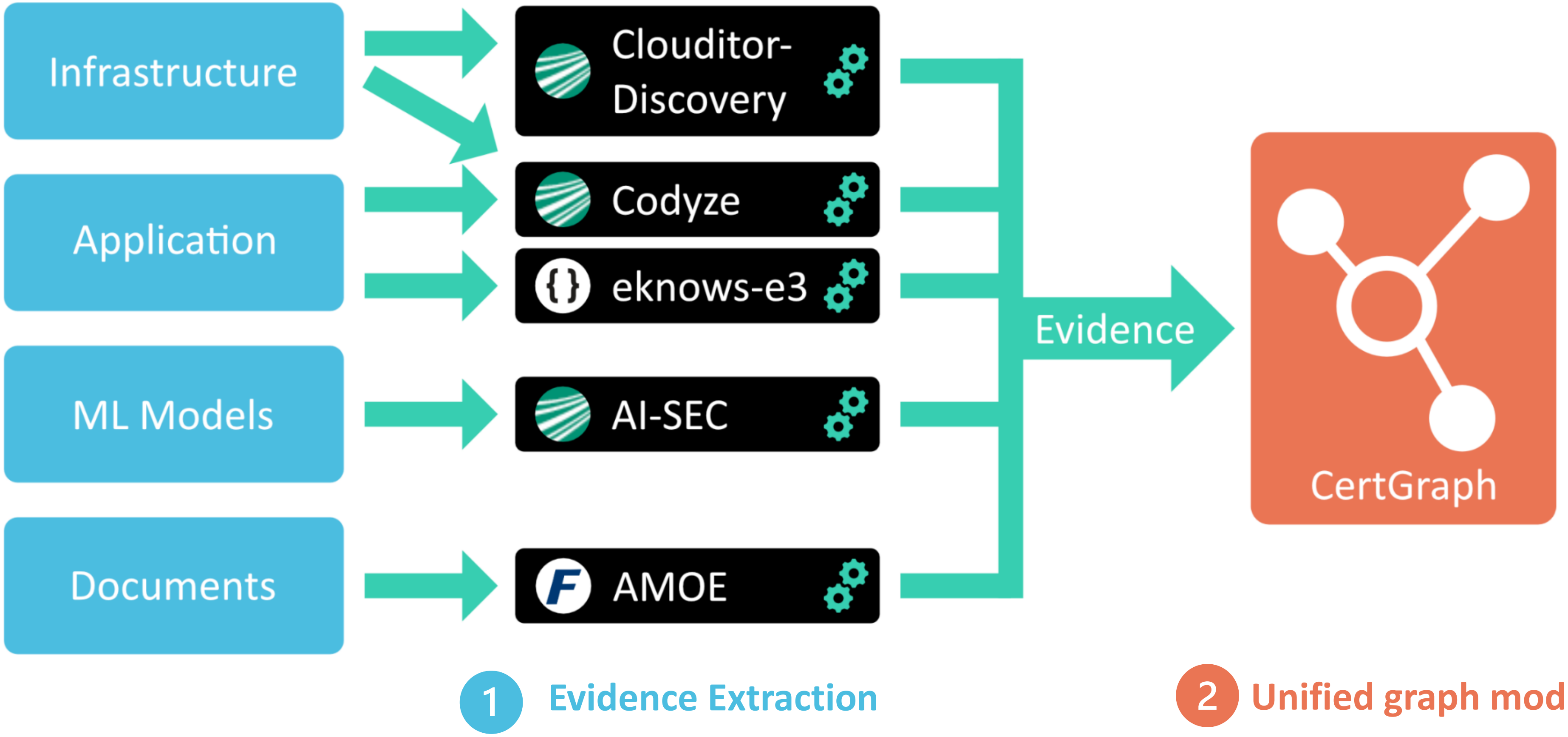
EMERALD UI/UX

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

INTEROP

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

EMERALD



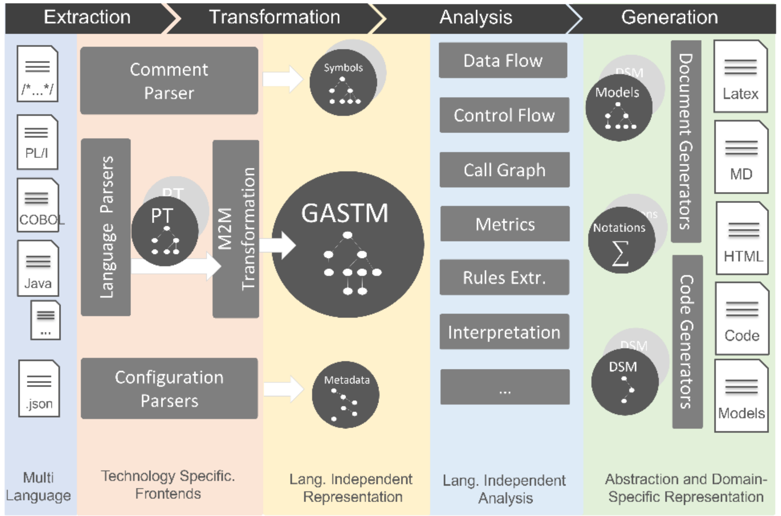
1 Provide next-generation evidence gathering tools based on a knowledge graph approach

Extraction from source code:

eknows-e3 Platform

- Static code analysis

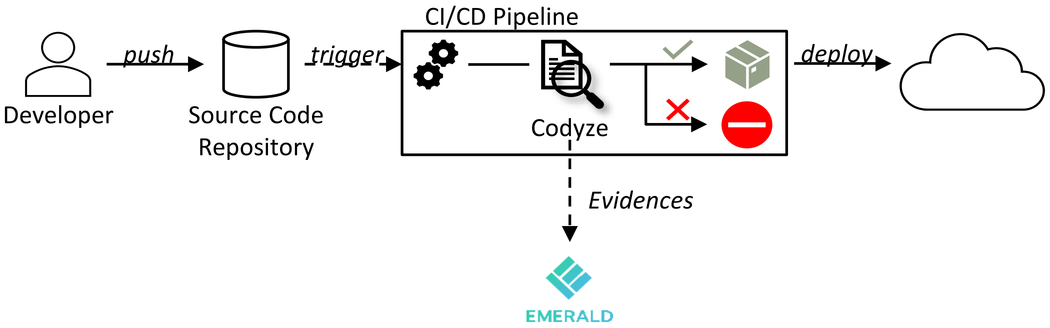
- Multi Language Support



Codyze

- Correct usage of libraries

- Integrated into CI/CD and IDEs



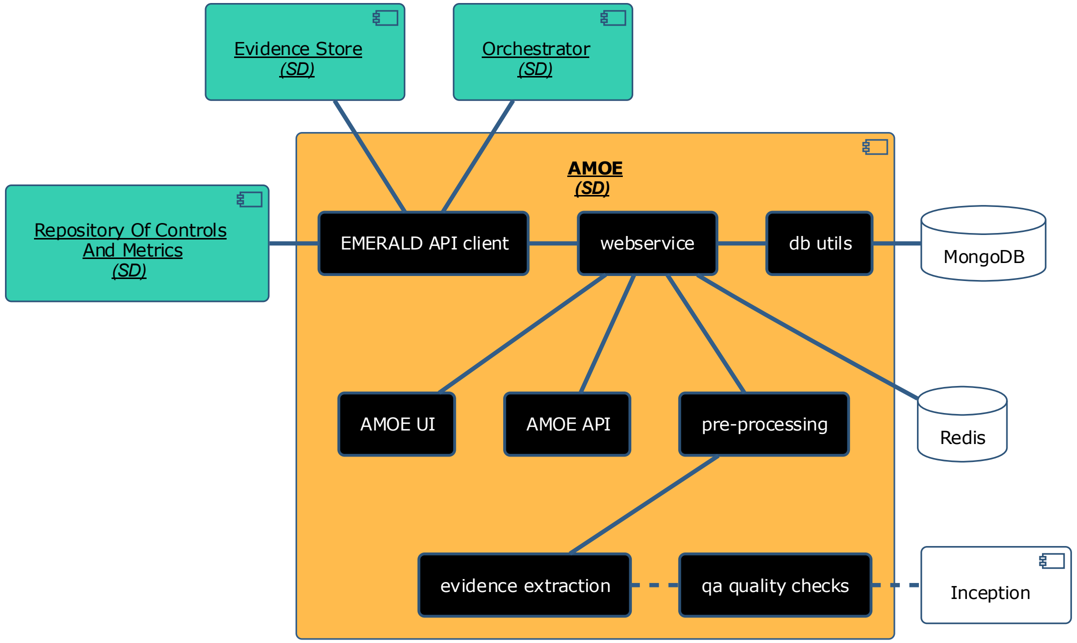
Extraction from documents:

AMOE

- PDF processing

- NLP and pre-trained AI models

- Policy Documents

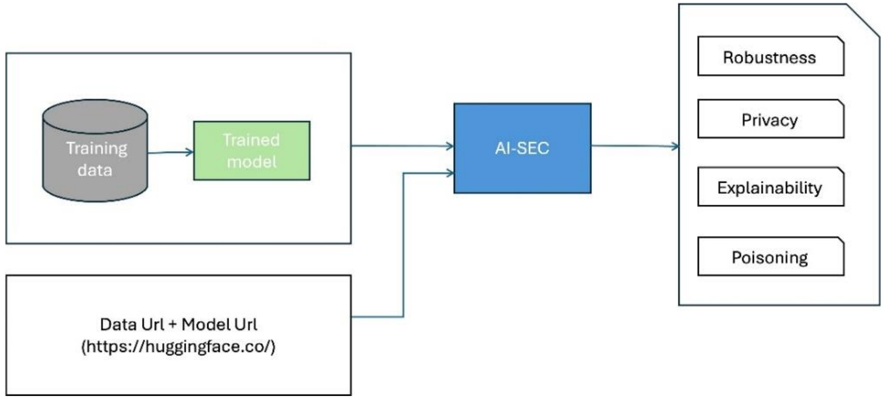


Extraction from ML models:

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

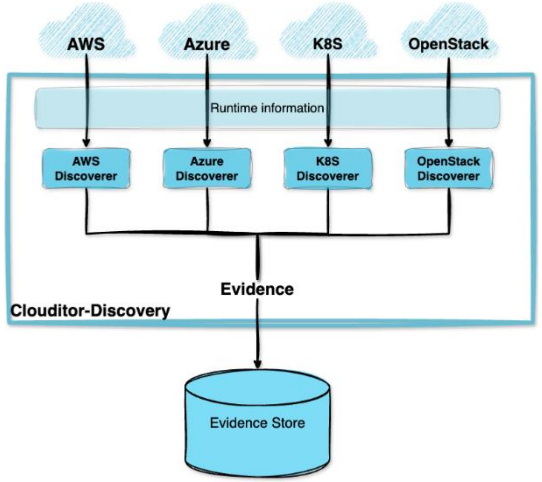
EMERALD

Extraction from Infrastructure:

Clouditor-Discovery

- Extract runtime Information from Cloud resources using Cloud providers APIs

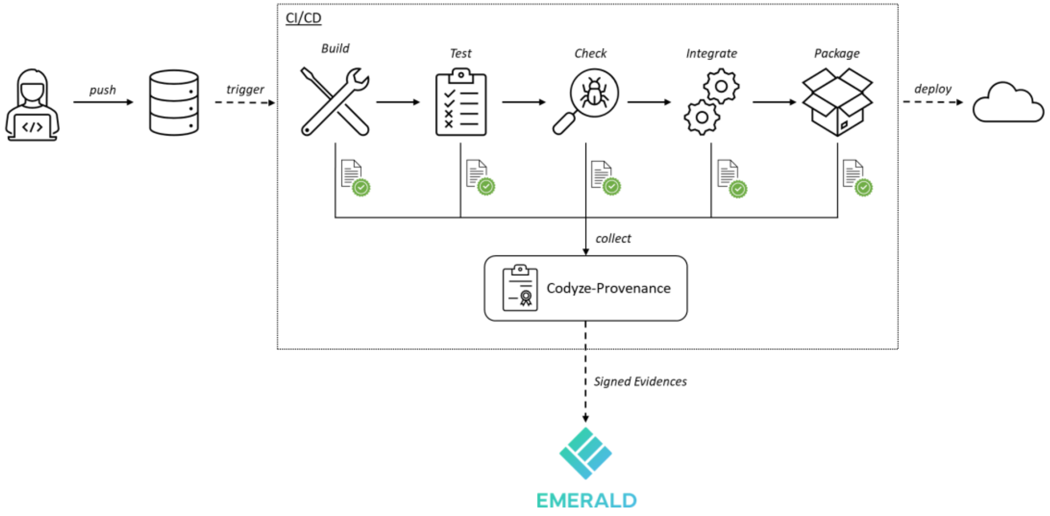
-Azure, AWS, Kubernetes, OpenStack



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

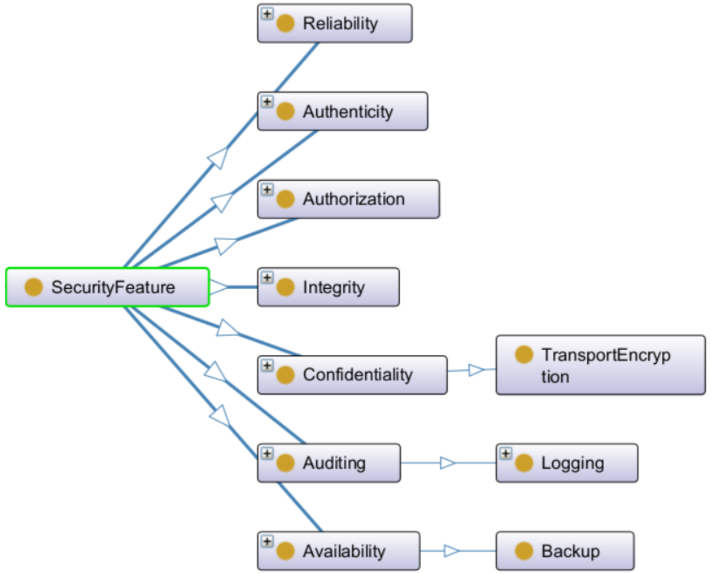
Evidence representation:

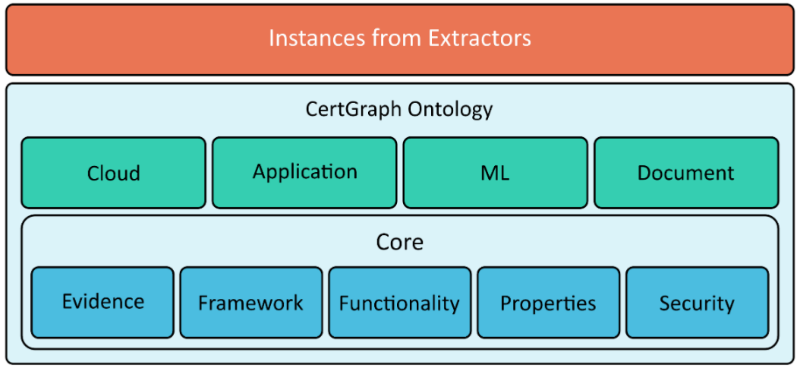
Cert-graph

- Multiple data sources

- Interconnected graph of evidence

- Modeled as ontology using Web Ontology Language (OWL)




Instances from Extractors

CertGraph Ontology

Cloud | Application | ML | Document

Core

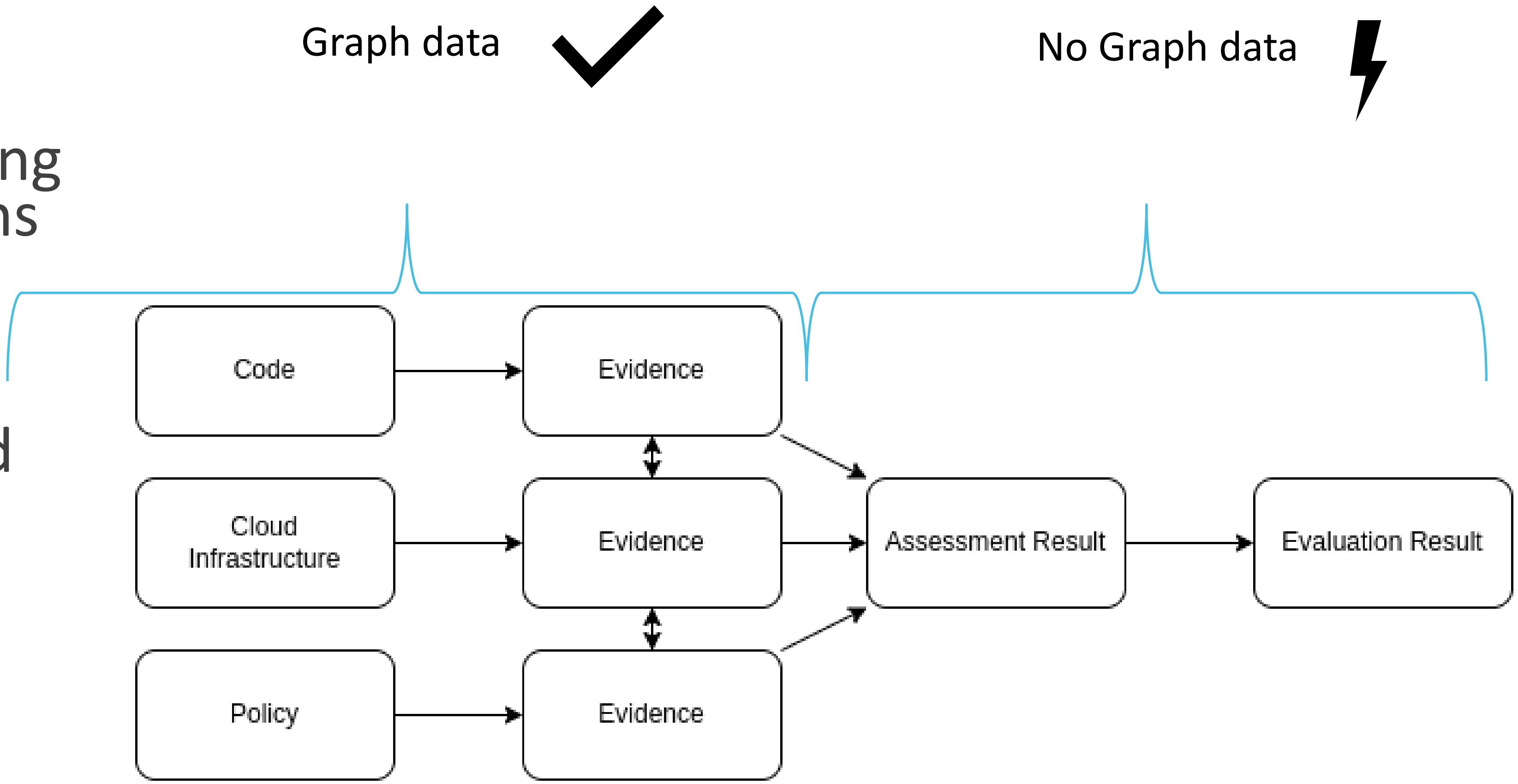
Evidence | Framework | Functionality | Properties | Security

Evidence store:

Hybrid database

- Use relational database that allows efficient storing of many data, e.g. millions of 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

EMERALD

Store controls and metrics:

RCM

- Multi-schema support: Controls from EUCS / BSI-C5 / AI-C4 / …

- Supports personalized schemas

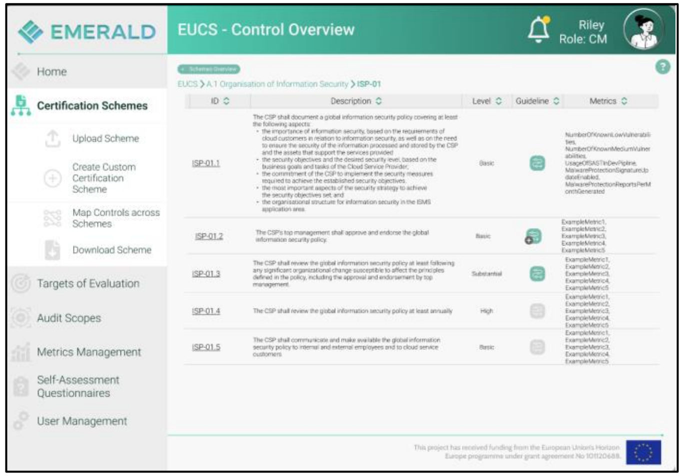
- Import/export mechanism (OSCAL)

Common Metrics Repository

- Provide realizable and reusable metrics

- 99 metrics mapped to schemes EUCS, BSI-C5 and BSI-AIC4

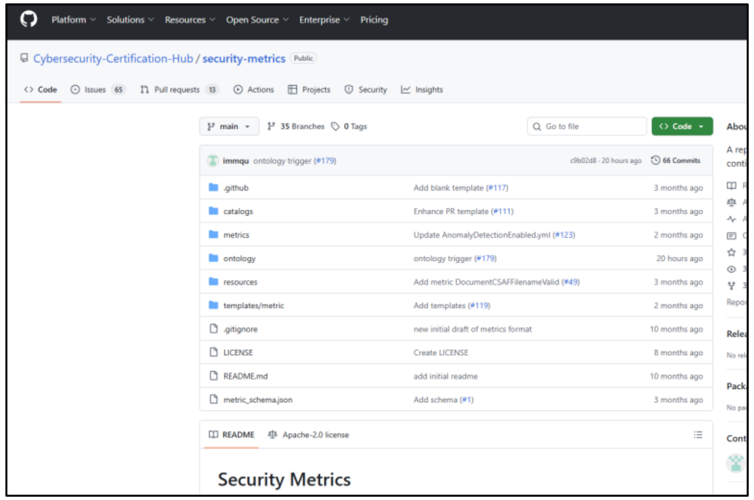
- 34 metrics mapped to more than one scheme



EUCS ❯ A.1 Organisation of Information Security ❯ ISP-01

ID	Description	Level	Guideline	Metrics
ISP-01.1	The CSP shall document a global information security policy covering at least the following aspects: • the importance of information security, based on the requirements of cloud customers in relation to information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the commitment of the CSP to implement the security measures required to achieve the established security objectives. • the most important aspects of the security strategy to achieve the security objectives set; and • the organisational structure for information security in the ISMS application area.	Basic		NumberOfKnownLowVulnerabilities, NumberOfKnownMediumVulnerabilities, UsageOfSASTInDevPipline, MalwareProtectionSignatureUpdateEnabled, MalwareProtectionReportsPerMonthGenerated
ISP-01.2	The CSP's top management shall approve and endorse the global information security policy.	Basic		ExampleMetric1, ExampleMetric2, ExampleMetric3, ExampleMetric4, ExampleMetric5
ISP-01.3	The CSP shall review the global information security policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management.	Substantial		ExampleMetric1, ExampleMetric2, ExampleMetric3, ExampleMetric4, ExampleMetric5
ISP-01.4	The CSP shall review the global information security policy at least annually	High		ExampleMetric1, ExampleMetric2, ExampleMetric3, ExampleMetric4, ExampleMetric5
ISP-01.5	The CSP shall communicate and make available the global information security policy to internal and external employees and to cloud service customers	Basic		ExampleMetric1, ExampleMetric2, ExampleMetric3, ExampleMetric4, ExampleMetric5

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



Cybersecurity-Certification-Hub / security-metrics Public

35 Branches 0 Tags

immqu ontology trigger (#179) c9b02d8 · 20 hours ago 66 Commits

.github	Add blank template (#117)	3 months ago
catalogs	Enhance PR template (#111)	3 months ago
metrics	Update AnomalyDetectionEnabled.yml (#123)	2 months ago
ontology	ontology trigger (#179)	20 hours ago
resources	Add metric DocumentCSAFFilenameValid (#49)	3 months ago
templates/metric	Add templates (#119)	2 months ago
.gitignore	new initial draft of metrics format	10 months ago
LICENSE	Create LICENSE	8 months ago
README.md	add initial readme	10 months ago
metric_schema.json	Add schema (#1)	3 months ago

Security Metrics

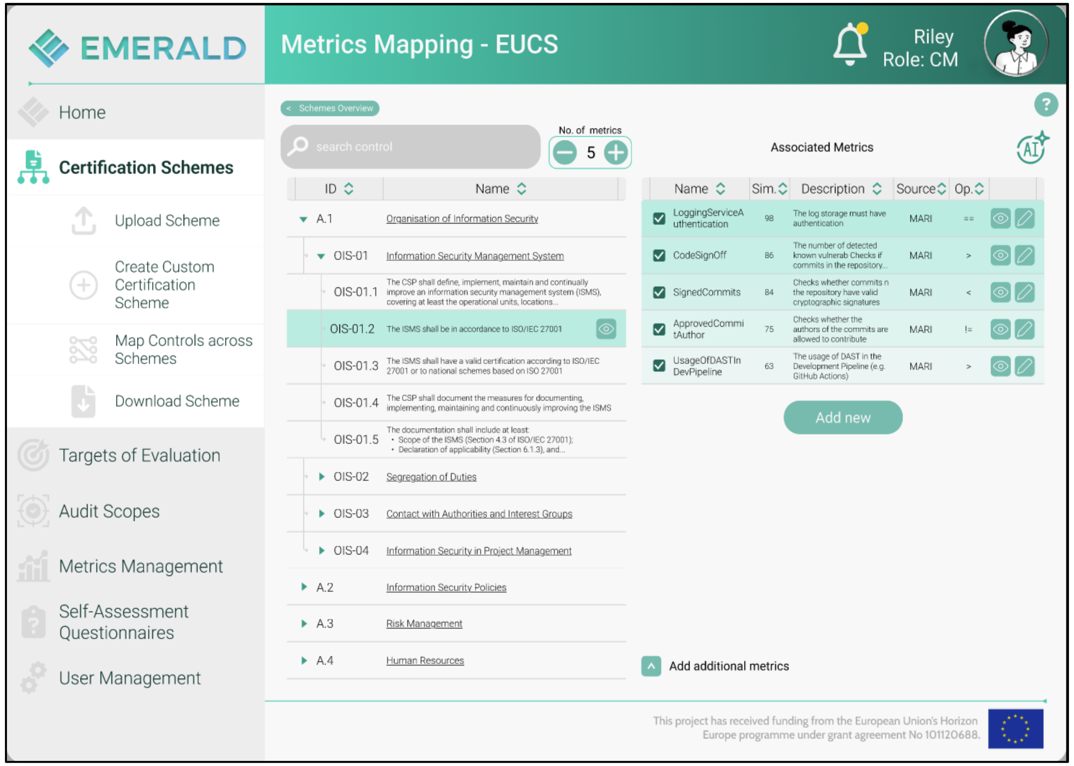
Metrics and controls associations:

MARI

- Automatically links metrics to controls

- Automatically links controls across multiple certification schemes

- The association exploits the textual descriptions of metrics and controls



Metrics Mapping - EUCS

ID	Name
A.1	Organisation of Information Security
OIS-01	Information Security Management System
OIS-01.1	The CSP shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations...
OIS-01.2	The ISMS shall be in accordance to ISO/IEC 27001
OIS-01.3	The ISMS shall have a valid certification according to ISO/IEC 27001 or to national schemes based on ISO 27001
OIS-01.4	The CSP shall document the measures for documenting, implementing, maintaining and continuously improving the ISMS
OIS-01.5	The documentation shall include at least: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and...
OIS-02	Segregation of Duties
OIS-03	Contact with Authorities and Interest Groups
OIS-04	Information Security in Project Management
A.2	Information Security Policies
A.3	Risk Management
A.4	Human Resources

Associated Metrics

	Name	Sim.	Description	Source	Op.
☑	LoggingServiceAuthentication	98	The log storage must have authentication	MARI	==
☑	CodeSignOff	86	The number of detected known vulnerab Checks if commits in the repository...	MARI	>
☑	SignedCommits	84	Checks whether commits n the repository have valid cryptographic signatures	MARI	<
☑	ApprovedCommitAuthor	75	Checks whether the authors of the commits are allowed to contribute	MARI	!=
☑	UsageOfDASTInDevPipeline	63	The usage of DAST in the Development Pipeline (e.g. GitHub Actions)	MARI	>

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

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

EMERALD

Metrics assessment and trustworthy compliance results

Clouditor Assessment & Evaluation

- Aggregation of assessment results for each control -> evaluation result

Clouditor Orchestrator

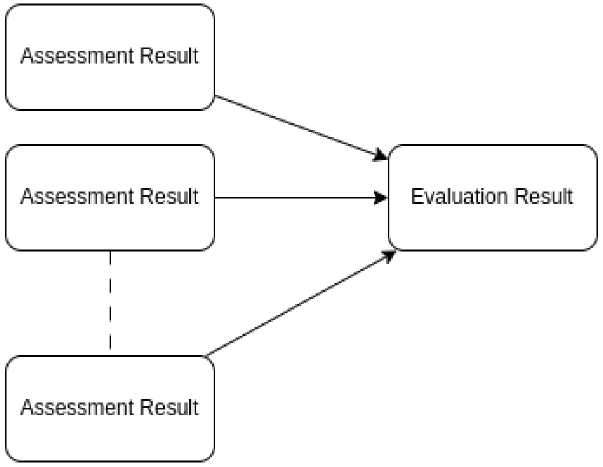
- Connects multiple components

- Compliance Decision (state machine)

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

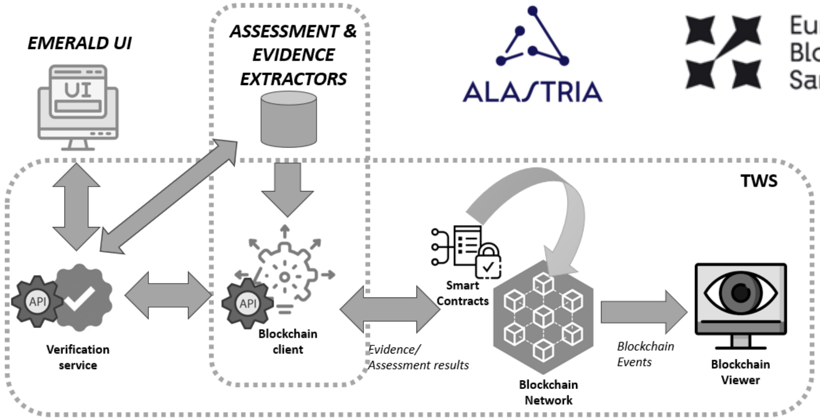


Assessment Result

Assessment Result

Assessment Result

Evaluation Result



ALASTRIA

European Blockchain Sandbox

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

EMERALD

User experience for complexity reduction

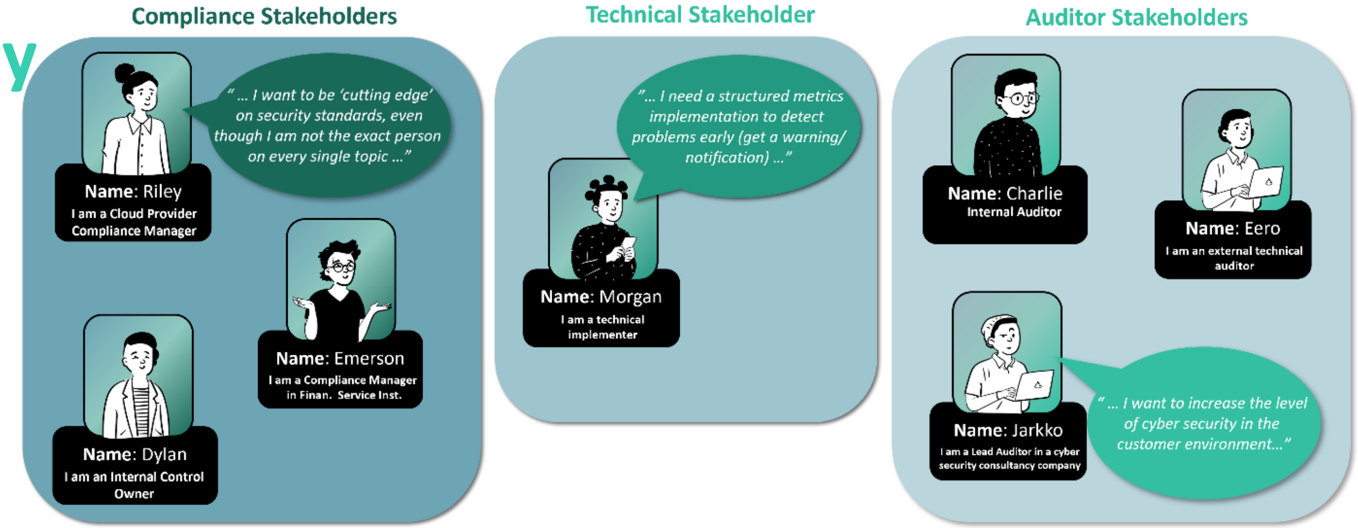
EMERALD UI/UX

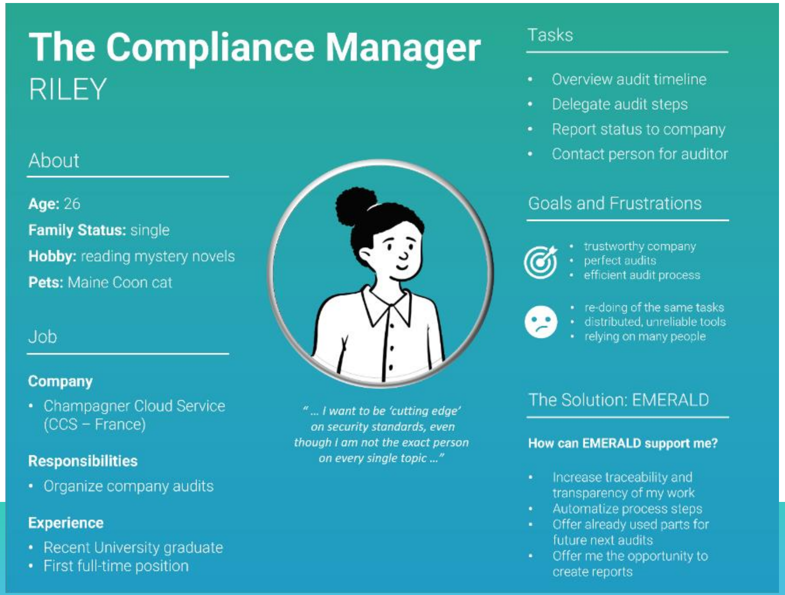
- User-centered requirements

- 7 Personas divided into 3 stakeholder groups

- Work process modelling: Developed 7 user personas with scenarios and user journeys to define interaction concepts and work processes.

- UI/UX design: Created paper and clickable mock-ups


Compliance Stakeholders
" … I want to be 'cutting edge' on security standards, even though I am not the exact person on every single topic …"
Name: Riley
I am a Cloud Provider Compliance Manager
Name: Emerson
I am a Compliance Manager in Finan. Service Inst.
Name: Dylan
I am an Internal Control Owner
Technical Stakeholder
"… I need a structured metrics implementation to detect problems early (get a warning/ notification) …"
Name: Morgan
I am a technical implementer
Auditor Stakeholders
Name: Charlie
Internal Auditor
Name: Eero
I am an external technical auditor
Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company
" … I want to increase the level of cyber security in the customer environment…"



The Compliance Manager

RILEY

About

Age: 26

Family Status: single

Hobby: reading mystery novels

Pets: Maine Coon cat

Job

Company

- Champagner Cloud Service (CCS – France)

Responsibilities

- Organize company audits

Experience

- Recent University graduate
- First full-time position

" … I want to be 'cutting edge' on security standards, even though I am not the exact person on every single topic …"

Tasks

- Overview audit timeline
- Delegate audit steps
- Report status to company
- Contact person for auditor

Goals and Frustrations

- trustworthy company
- perfect audits
- efficient audit process

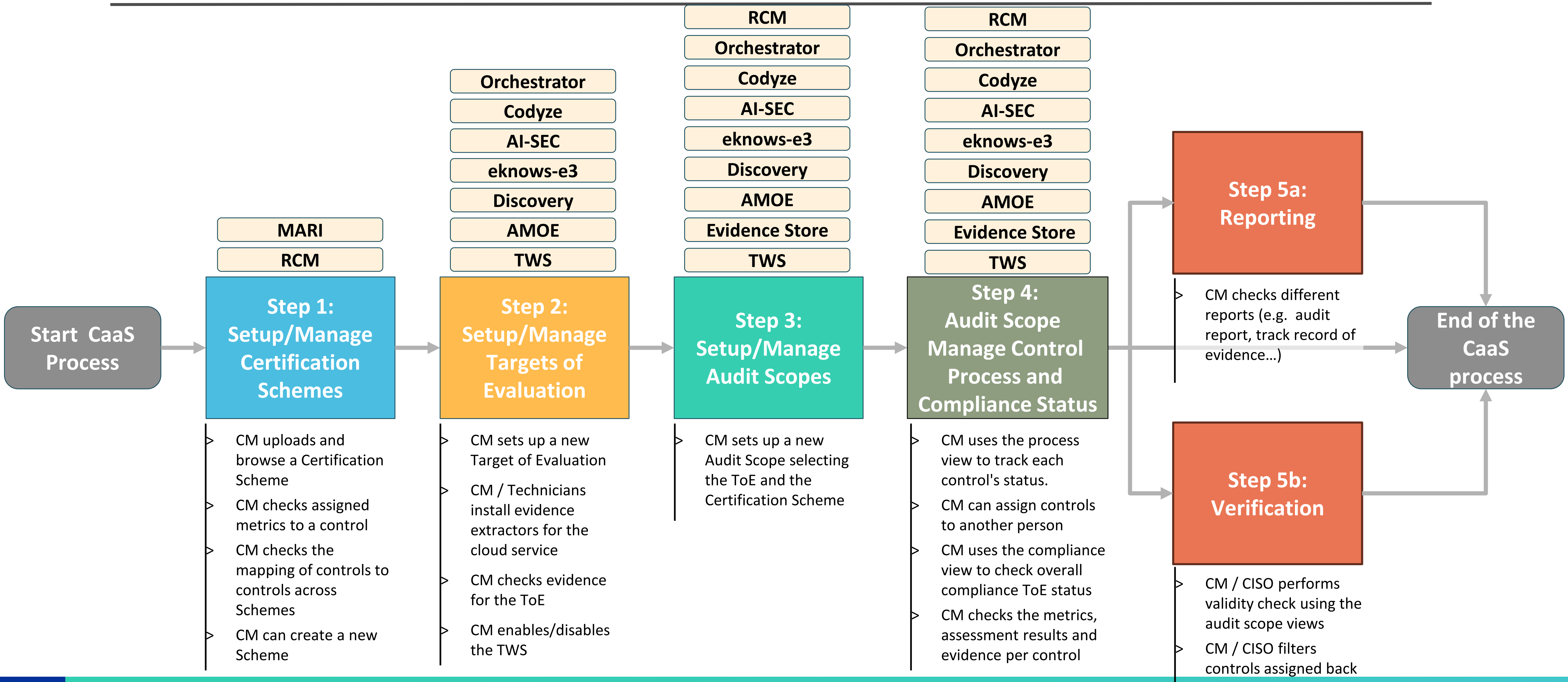
- re-doing of the same tasks
- distributed, unreliable tools
- relying on many people

The Solution: EMERALD

How can EMERALD support me?

- Increase traceability and transparency of my work
- Automatize process steps
- Offer already used parts for future next audits
- Offer me the opportunity to create reports

EMERALD CaaS: UI Workflow



Start CaaS Process

MARI
RCM

Step 1: Setup/Manage Certification Schemes

- CM uploads and browse a Certification Scheme
- CM checks assigned metrics to a control
- CM checks the mapping of controls to controls across Schemes
- CM can create a new Scheme

Orchestrator
Codyze
AI-SEC
eknows-e3
Discovery
AMOE
TWS

Step 2: Setup/Manage Targets of Evaluation

- CM sets up a new Target of Evaluation
- CM / Technicians install evidence extractors for the cloud service
- CM checks evidence for the ToE
- CM enables/disables the TWS

RCM
Orchestrator
Codyze
AI-SEC
eknows-e3
Discovery
AMOE
Evidence Store
TWS

Step 3: Setup/Manage Audit Scopes

- CM sets up a new Audit Scope selecting the ToE and the Certification Scheme

RCM
Orchestrator
Codyze
AI-SEC
eknows-e3
Discovery
AMOE
Evidence Store
TWS

Step 4: Audit Scope Manage Control Process and Compliance Status

- CM uses the process view to track each control's status.
- CM can assign controls to another person
- CM uses the compliance view to check overall compliance ToE status
- CM checks the metrics, assessment results and evidence per control

Step 5a: Reporting

- CM checks different reports (e.g. audit report, track record of evidence…)

Step 5b: Verification

- CM / CISO performs validity check using the audit scope views
- CM / CISO filters controls assigned back

End of the CaaS process

Outline for the session

Ice breaking session : General topics and concepts	5 min
Cybersecurity certification for the Computing Continuum Future Challenges and opportunities	10 min
EMERALD: Towards Automatized Compliance as a Service for the Computing Continuum	45 min
Open discussion and questions	30 min

GET IN TOUCH

www.emerald-he.eu

@emerald-he-project

emerald-he-project

Scan me!