EMERALD

# Deliverable D5.1

# Pilot definition, set-up & validation plan

| | |
|---|---|
| **Editor(s):** | Olivia Kagerer (FABA) |
| **Responsible Partner:** | Fabasoft R&D GmbH |
| **Status-Version:** | Final - v1.0 |
| **Date:** | 31.07.2024 |
| **Type:** | R |
| **Distribution level (SEN, PU):** | PU |

| | |
|---|---|
| **Project Number:** | 101120688 |
| **Project Title:** | EMERALD |

| | |
|---|---|
| **Title of Deliverable:** | D5.1 Pilot definition, set-up & validation plan |
| **Due Date of Delivery to the EC** | 31.07.2024 |

| | |
|---|---|
| **Workpackage responsible for the Deliverable:** | WP5 - EMERALD operational and financial Pilots |
| **Editor(s):** | Fabasoft R&D GmbH |
| **Contributor(s):** | Mika Leskinen (NIXU), Jordi Guijarro (ONS), Ramon Martín de Pozuelo (CXB), Natalia Sobieska (CF), Netsanet Haile Gebreyesus (IONOS), Lukas Ruckenstuhl (FABA) |
| **Reviewer(s):** | Angela Fessl (KNOW)<br>Cristina Martínez (TECNALIA) |
| **SAB Reviewers:** | Samu Nisula (NIXU)<br>Constantino Vázquez (ONS)<br>Mario Maawad (CXB)<br>Daniela Greb (FABA)<br>Tomasz Aniszewski (CF)<br>Ali Nikouka (IONOS) |
| **Approved by:** | All Partners |
| **Recommended/mandatory readers:** | WP1, WP2 WP3, WP4 |

| | |
|---|---|
| **Abstract:** | Initial version of the report on Pilot set-up, validation plan of the user interaction concept, elicited requirements, and list of KPIs to measure the impact |
| **Keyword List:** | Pilots, Validation Strategy, Requirements, KPIs, Impact Analysis |
| **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. |

# Document Description

| Version | Date | Modifications Introduced | |
|---|---|---|---|
| | | Modification Reason | Modified by |
| v0.1 | 08.02.2024 | First draft version ToC | FABA |
| v0.2 | 02.05.2024 | Final version of ToC | FABA |
| v0.3 | 16.05.2024 | Finalized validation plan | FABA, NIXU |
| v0.4 | 03.07.2024 | Finalized contribution pilot 4 | FABA, ONS, CXB |
| v0.5 | 03.07.2024 | Finalized contribution pilot 3 | FABA |
| v0.6 | 05.07.2024 | Finalized contribution pilot 1 | IONOS |
| v0.7 | 05.07.2024 | Finalized contribution pilot 2 | CF |
| v0.8 | 12.07.2024 | QA and SAB review | KNOW |
| v0.9 | 24.07.2024 | Address the comments from the QA and SAB review | IONOS, CF, FABA, CXB, ONS |
| v1.0 | 31.07.2024 | Submitted to the European Commission | TECNALIA |

# Table of contents

## List of tables

## List of figures

## Terms and abbreviations

| | |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| AI | Artificial Intelligence |
| AIC4 | AI Cloud Service Compliance Criteria Catalogue |
| AMOE | Assessment and Management of Organizational Evidence |
| API | Application Programming Interface |
| AWS | Amazon Web Services |
| BDR | Business-Driven Requirements |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| C5 | Cloud Computing Compliance Criteria Catalogue |
| CaaS | Certification-as-a-Service |
| CF | CloudFerro |
| CI/CD | Continuous Integration / Continuous Delivery |
| CISO | Chief Information Security Officer |
| CSA or EU CSA | EU Cybersecurity Act |
| CSP | Cloud Service Provider |
| CSV | Comma-separated values |
| DLR | Data Retrieval Language |
| DoA | Description of Action |
| ECMWF | European Centre for Medium-Range Weather Forecasts |
| ESA | European Space Agency |
| EUCS | European Cybersecurity Certification Scheme for Cloud Services |
| EUMETSAT | European operational satellite agency for monitoring weather, climate and the environment |
| GA | General Assembly |
| IaaS | Infrastructure-as-a-Service |
| ISO | International Organization for Standardization |
| IT | Information Technologies |
| ITS | Information Technology Services |
| KPI | Key Performance Indicator |
| KR | Key Result |
| MARI | Mapping Assistant for Requirements with Intelligence |
| ML | Machine Learning |
| NPS | Net Promoter Score |
| OSCAL | Open Security Controls Assessment Language |
| PaaS | Platform-as-a-Service |
| PGC | Plan General de Contabilidad (chart of accounts) |
| PSD2 | Payment Services Directive2 |
| RCM | Repository of Controls and Metrics |
| RFQ | Request For Quotation |
| SaaS | Software-as-a-Service |
| SIEM | Security Information and Event Management |
| SUS | System Usability Scale |
| TWS | Trustworthiness System |
| UI | User Interface |

| | |
|---|---|
| UNED | Universidad Nacional de Educación a Distancia (National University of Distance Education) |
| UVP | Unique Value Proposition |
| UX | User Experience |
| VM | Virtual Machine |
| WP | Work Package |

# Executive Summary

This deliverable D5.1 defines the EMERALD pilots as well as their set-up. Additionally, it introduces the validation plan of the EMERALD framework and its pilots.

Through the definition of the pilots, specifically their respective business-driven requirements and the Key Performance Indicators (KPIs), the deliverable aims to support the technical work packages (WP1-WP4) of EMERALD in gaining a deeper understanding of the pilot goals and requirements. This is intended to ease the communication within the EMERALD project, specifically between the technical and non-technical work packages.

It is intended that the validation plan will serve to generate iterative feedback to the technical work packages and the pilots themselves. Specifically with the Stage-Gate-Process, it will be ensured that the EMERALD framework can provide support for the automation of audits and that the pilots provide the necessary data and inputs for the EMERALD component owners.

As a result, the main sections of this deliverable are as follows:

- Pilot definition and set-up, which introduces each pilot and its respective goals. This includes a list of business-driven requirements and pilot KPIs for each EMERALD pilot.
- Validation plan, which supports the generation of iterative feedback for the implementation of the EMERALD framework, as part of Task 5.2 and Task 5.3. This includes the plan for the impact analysis, which details the approach for measuring and analysing the impact of the EMERALD project, which will be followed in Task 5.4.

The future deliverables of WP5 will be based on this deliverable D5.1, as the pilots will integrate the EMERALD framework and will supply feedback by following the validation plan. These results will be reported in D5.2 and D5.3 (Pilot Category I), as well as in D5.4 and D5.5 (Pilot Category II). In D5.6, the results of the impact analysis will be presented.

# 1 Introduction

This deliverable introduces the four pilots of EMERALD and the validation plan, in order to help the technical work packages (WP1-WP4) to better understand the objectives and requirements of the pilots.

## 1.1 About this deliverable

This deliverable D5.1 presents the pilot definition and set-up for each of the EMERALD pilots. Additionally, it introduces the validation plan and details its application. Lastly, it includes the plan for measuring the impact of the EMERALD framework through the validation plan.

The set-up and definition of the pilots allows an in-depth understanding of their respective goals and overall approach towards the EMERALD project. This creates a source of truth and consequently supports the communication between technical and non-technical work packages, as relevant information is documented and can be referenced by all. To achieve this, each pilot presents the following information:

- Current practices and expected benefits through the application of the EMERALD framework
- Clear definition of the pilot from various perspectives, such as the planned workflow in the pilot, the technical perspective and system architecture and the communication between various actors in the pilot. The goals of the pilot are then summarized in the pilot KPIs and business-driven requirements.
- Planned approach for the integration of the EMERALD framework into the pilot, detailing the certification targets and the use of each EMERALD component.

The validation plan presents the methodology for the validation of the EMERALD framework and its pilots. This methodology includes the following processes:

- Stage-gate-process, which ensures that the EMERALD framework can support an audit from start to finish, and that all relevant information is provided by the pilots.
- Impact analysis, which uses several approaches for measuring the impact of the EMERALD framework on the pilots. This includes the analysis of value statements and customer satisfaction, as well as the measurement of the impact KPIs and a validation through stakeholders.
- Fulfilment tracking of business-driven requirements and analysis of the pilot KPIs, which respectively ensure that the requirements are fulfilled and that the KPIs can be achieved.
- User Experience (UX) validation which measures how useful the implemented EMERALD framework, and specifically the EMERALD user interface (UI), is perceived by the users and which generates feedback towards the EMERALD UI regarding any usability issues.

The validation plan will be followed by the pilots with the support of the technical partners throughout the duration of the project. The plan specifies a schedule for when the pilots are expected to create and report their feedback to the technical work packages in the project.

## 1.2 Document structure

This deliverable is split into two main sections. Section 2 introduces the pilots in separate subsections with a similar structure, as described above. Section 3 introduces the validation plan for the duration of the EMERALD project. Each of these sections are independent of each other. The first section can be seen as source of truth for the pilot and their further plans, while the second can be seen as guideline for the validation plan, including the impact analysis.

The Deliverable is summarized in Section 4. The business-driven requirements, as defined by the pilots, can be found in *APPENDIX A: Business-driven requirements*. The KPIs and Impact KPIs, as defined in the DoA can be found in *APPENDIX B: KPIs and Impact KPIs*, and the approach to measure the Impact KPIs can be found in *APPENDIX C: Impact KPI measurement example*.

# 2 Pilot Definition and Set-Up

The four pilots of EMERALD serve as realistic use cases, as each pilot partner is a potential user of EMERALD. As such, the pilots can provide examples for a real-world application of EMERALD and test data, which can be used for fine tuning the evidence extraction tools and improving the quality of their results. To showcase an end-to-end audit scenario, each of the EMERALD pilots will follow a stage-gate-process (see Section 3.1) in collaboration with an auditor. In addition, each pilot will follow the validation plan with iterative feedback (see Section 3) to ensure reduced complexity and increased user acceptance.

The pilots will describe a path to integrate the EMERALD tools into European cloud service providers, under the consideration of technical and organizational restrictions which apply during the application of the EMERALD framework. The first three pilots are part of Category I, and the fourth pilot is in Category II. While the pilots of Category I aim for demonstrating Certification-as-a-Service (CaaS) with EMERALD for public cloud services for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), Category II aims for the certification of hybrid cloud-edge environments in the financial sector.

This section introduces the definition and set-up of each pilot. For this purpose, the current situation and the expected benefits of the EMERALD framework are presented, followed by a detailed definition of the pilot, including business-driven requirements and pilot KPIs for the validation. Lastly, each pilot describes the approach for the integration of the EMERALD framework, detailing the evidence sources for the certification of the pilots and the application of the components of the EMERALD framework.

## 2.1 Pilot 1: IONOS

Pilot 1 is designed to address specific challenges in the public cloud domain. This pilot is strategically poised at IONOS, leveraging their robust infrastructure and broad market reach to assess and validate the implementation of CaaS methodologies. The goal is to streamline and enhance the security certification processes that are currently fragmented and cumbersome, thereby setting a benchmark for agile, continuous certification in cloud computing.

### 2.1.1 Introduction and Motivation

Pilot 1 aims to implement and validate the EMERALD framework, specifically designed to facilitate the auditing and certifying process in a cloud environment. By deploying this advanced framework, pilot 1 seeks to automate the tracking and reporting of compliance across a vast array of services, ensuring they adhere to the latest regulations without manual overhead. The goal is to streamline these processes, thus reducing the time and resources traditionally required for compliance activities, which are often cumbersome and error-prone.

The motivation behind pilot 1 lies in the growing complexity and dynamic nature of cloud computing, which demands a more agile and scalable approach to compliance and security management. As cloud technologies evolve and regulatory requirements become more stringent, traditional methods of certification prove inadequate in terms of both efficiency and efficacy. IONOS's participation in pilot 1 not only positions the company as a leader in secure cloud solutions but also demonstrates a proactive stance in addressing the challenges faced by cloud service providers today. Through this pilot, IONOS aims to showcase its commitment to security and compliance, enhancing customer trust and paving the way for new business opportunities in a highly competitive market.

#### *2.1.1.1 Current Practice and Problem Statement (before EMERALD)*

The landscape of cloud security certification in Europe currently displays significant fragmentation, lacking a cohesive approach as emphasized by the European Union's Cybersecurity Act[1]. Efforts are underway to rectify this through the proposed European Cybersecurity Certification Scheme (EUCS)[2]. Despite the increasing reliance on cloud technologies, there remains a notable deficiency in the regular and systematic certification of these services. This shortfall impacts trust and compliance, especially for Small and Medium Enterprises (SMEs) and sectors with strict regulatory demands. Traditional certification models, typically static, struggle to adapt to the dynamic and evolving nature of cloud services, including rapid changes in configurations and threat landscapes. This problem is exacerbated by the disjointed nature of security standards and the absence of a consistent framework for validating ongoing compliance.

Public cloud providers experience challenges due to the diverse landscape of cloud security certification, which has not yet fully adapted to the rapid evolution of cloud technologies. To address this, there is a need for a shift away from traditional, manual documentation methods, such as spreadsheets, which can be inefficient and susceptible to errors. The preparation for compliance audits typically involves the engagement of consultancy services, an approach that, while effective, often results in increased operational costs and can delay the introduction of new services. Moreover, the lack of uniformity in certification schemes across Europe poses challenges in developing a standardized compliance strategy, occasionally leading to the isolated

[1] https://eur-lex.europa.eu/eli/reg/2019/881/oj

[2] https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework

use of assessment tools that can impact the seamless interoperability and integration of services.

In contrast, the EMERALD project's approach, set to be demonstrated in pilot 1, seeks to mitigate these issues by introducing a unified certification graph and ongoing certification processes. This method aligns with the EU's strategy for a digital single market and incorporates emerging standards like the Open Security Controls Assessment Language[3] (OSCAL) to foster greater standardization and interoperability across different cloud services.

#### 2.1.1.2 Expected Benefits (after EMERALD)

The implementation of pilot 1 in IONOS aims to deliver several transformative benefits:

- Enhanced Security Assurance: Continuous certification will provide ongoing assurance of compliance with evolving security standards, reducing the incidence and impact of security breaches.
- Reduced Certification Overheads: By automating and integrating certification processes, the time and cost involved in achieving and maintaining compliance will significantly decrease.
- Boosted Market Confidence: Establishing a transparent and reliable certification process will increase trust among existing and potential customers, particularly those from regulated sectors.
- Scalability and Flexibility: The pilot will demonstrate a scalable model for continuous certification that can adapt to various cloud architectures and services, promoting broader adoption across the industry.

### 2.1.2 Pilot definition

The pilot 1 definition outlines the structure and key participants of the initiative, detailing their roles and responsibilities within the project. This section ensures that all stakeholders are aligned with the pilot's objectives, facilitating effective collaboration and successful execution.

#### 2.1.2.1 Pilot Diagram

Figure 1 presents a high-level diagram illustrating the relationships and workflows between various stakeholders involved in pilot 1. The diagram serves as a visual guide to the operational structure and the interaction dynamics among the participants. The roles of the stakeholders are described as follows:

- IONOS Management Team: Oversee the pilot's execution, ensuring alignment with company objectives and providing strategic direction.
- Cloud Service Providers (CSPs): Implement cloud services that need to be certified under the new continuous certification framework, provide feedback on system operations, and adjustments needed to meet certification requirements.
- Cloud Customers (End-Users): Act as beneficiaries of the certified cloud services, provide requirements for service levels and security features, and give feedback on the service efficacy.
- EMERALD Project Team: Develop and manage the CaaS framework, coordinate among different stakeholders, ensure the pilot aligns with the project's broader goals, and handle the integration of tools and processes for continuous certification.
- Regulatory Bodies: Provide compliance and regulatory guidelines that the certification must meet.

[3] https://pages.nist.gov/OSCAL/

- Cybersecurity Experts: Design and validate the security aspects of the cloud services being offered, ensuring that they meet the stringent criteria set out by both IONOS and regulatory standards.
- Auditors: Continuously monitor and evaluate the cloud services against established certification standards, report compliance levels, and suggest improvements.
- Technology Providers: Supply the necessary software, infrastructure, and technological support required to implement the pilot, including updates and maintenance.
- Standardization Agencies: Ensure the certification processes adhere to international and European standards, contributing to framework development and adjustment.

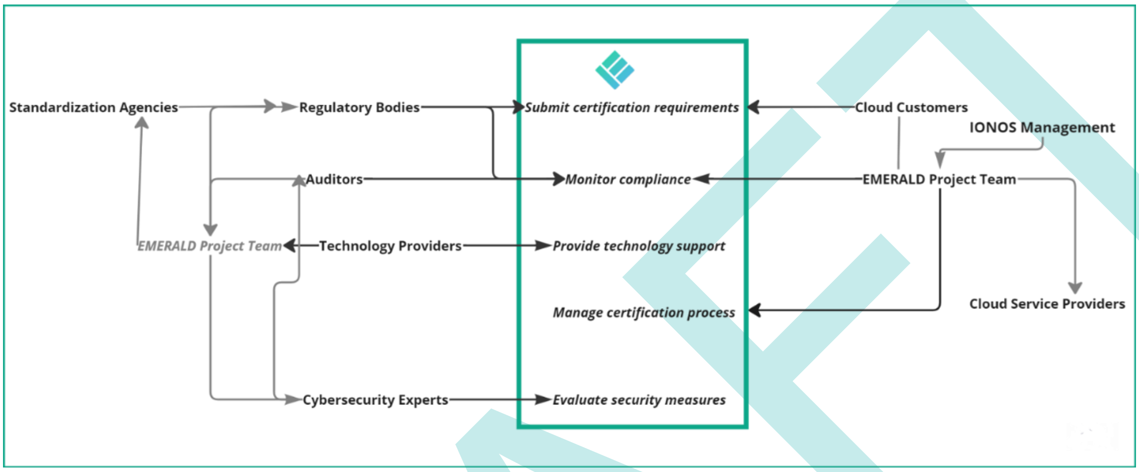


*Figure 1. Operational structure of pilot 1*

#### 2.1.2.2 Pilot workflow

This section describes the sequential phases of pilot 1, from preparation through to review and compliance assurance. Each phase is crucial for the pilot's success, detailing specific tasks, stakeholder involvement, and expected outcomes.

**Preparation Phase**

- Stakeholder Alignment: Engage all relevant stakeholders, including IONOS management, cloud service providers, regulatory bodies, and auditors, to ensure alignment on the project's objectives and responsibilities.
- Infrastructure Assessment: Evaluate the existing cloud infrastructure and technologies to determine the starting point for the pilot.
- Requirement Gathering: Collect detailed requirements from cloud customers, regulatory requirements from agencies, and input from cybersecurity experts to define the scope and goals of the certification framework.

**Design Phase**

- Framework Design: The EMERALD project team designs the continuous certification framework, which includes defining the certification process, criteria, and continuous monitoring mechanisms.
- Tool Integration: Select and integrate tools for automated evidence collection, security assessment, and compliance monitoring, such as Codyze for code analysis or AMOE for organizational evidence management.
- Pilot Design: Design the specific pilot test cases and scenarios that will validate the effectiveness of the continuous certification process.

**Implementation Phase**

- Deployment: Implement the designed framework and tools within the IONOS cloud environment, ensuring all components are properly integrated and functional.
- Training: Train the personnel involved in the pilot, including auditors and technical staff, on the new tools and processes.

**Testing and Validation Phase**

- Pilot Testing: Run the pilot test cases to validate the functionality and effectiveness of the continuous certification process.
- Feedback Collection: Gather feedback from all stakeholders, including cloud customers and technology providers, to assess the pilot's performance.
- Adjustments and Optimization: Make necessary adjustments based on feedback and initial testing outcomes to optimize the certification process.

**Review and Compliance Assurance Phase**

- Compliance Checks: Perform thorough compliance checks to ensure that all certification requirements are met and maintained throughout the pilot.
- Documentation: Document all processes, findings, and compliance statuses in detailed reports for internal and external use.
- Pilot Evaluation: Evaluate the overall success of the pilot based on predefined KPIs and success criteria.

#### 2.1.2.3 Technical perspective and system architecture

To enhance the reliability and performance of the EMERALD integration, several IONOS services will be utilized. *IONOS Kubernetes and Container Registry* will host a microservices architecture, ensuring scalable deployment of all EMERALD components. Kubernetes orchestration will facilitate seamless interactions between components, while the Container Registry will manage the storage and distribution of container images. *IONOS Cloud Storage and Database Solutions* will support the data storage needs of the RCM and TWS components, providing high-performance, scalable, and secure storage solutions necessary for managing large volumes of compliance data and evidence. *IONOS Networking Solutions* will ensure secure and reliable connectivity between the deployed components, safeguarding data in transit and ensuring compliance with data protection regulations. Figure 2 shows a high-level architecture of pilot 1.

The proposed integration strategy is designed to optimize the functionality of the EMERALD components within the IONOS cloud, ensuring that pilot 1 not only meets but exceeds its operational objectives, delivering efficient, secure, and compliant cloud services.

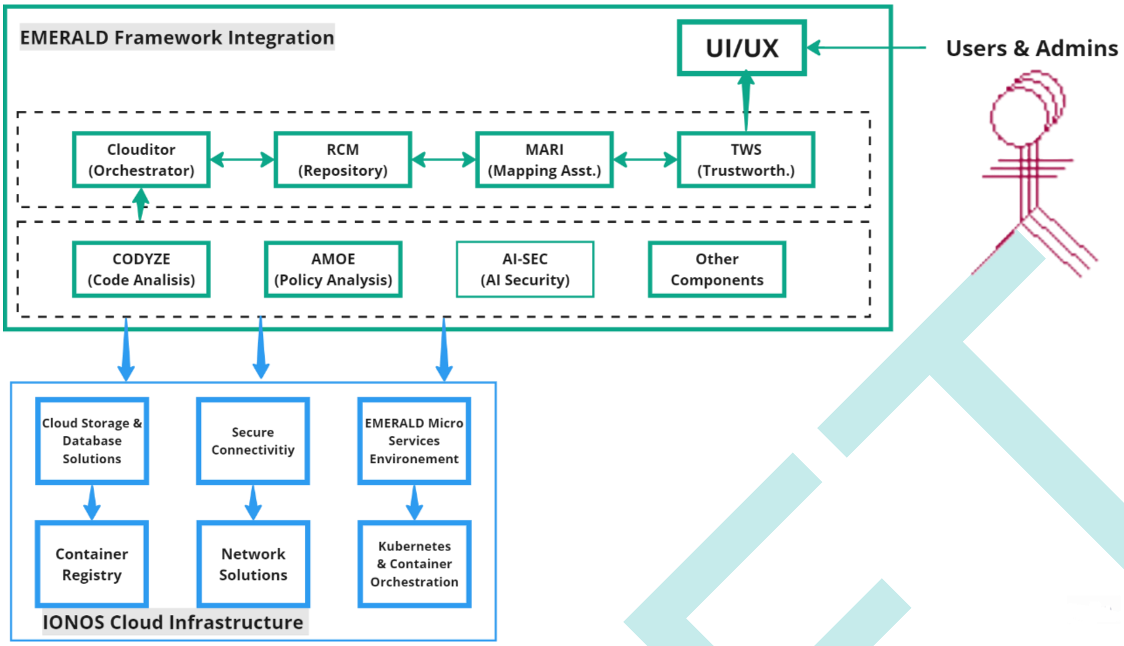


*Figure 2. High level Architecture of pilot 1*

### 2.1.2.4 Security controls and measures

Pilot 1 is set to create a segregated environment within the IONOS cloud infrastructure, specifically designed to house all EMERALD components—Clouditor, TWS, MARI, RCM, AMOE, Codyze, AI-SEC, and the EMERALD UI/UX—deployed as microservices. This isolation ensures that the operational integrity and compliance are maintained separate from regular business operations. To guarantee the security of this architecture, a comprehensive security penetration test will be executed to detect and mitigate any vulnerabilities, enhancing the security framework before the system goes live.

Key security measures include implementing advanced encryption and role-based access controls (RBAC) across all components. Access will be strictly managed to ensure that only authorized personnel, such as compliance managers, system administrators, developers, and auditors, can access specific functionalities based on their roles. Additionally, continuous monitoring will be employed using IONOS's own tools to oversee the performance and health of the components, allowing for proactive maintenance and updates to security and functionality as needed. This approach ensures a robust, secure, and compliant deployment of the EMERALD components in pilot 1.

### 2.1.2.5 Communication and workflow diagram

The sequence diagram below (Figure 3) illustrates the integration and workflow of the EMERALD framework within the IONOS cloud for Pilot 1, focusing on evidence extraction and storage processes. It begins with Clouditor initiating the evidence collection from source code repositories and organizational policy documents. The collected code and policy documents are then processed by Codyze for static code analysis and AMOE for policy compliance assessment, respectively. The results from these analyses are stored in the Trustworthiness System (TWS) for secure, long-term storage, while also updating the Repository of Controls and Metrics (RCM) with the latest compliance metrics and controls. Finally, Clouditor compiles all the results into comprehensive compliance reports for internal and external audits.

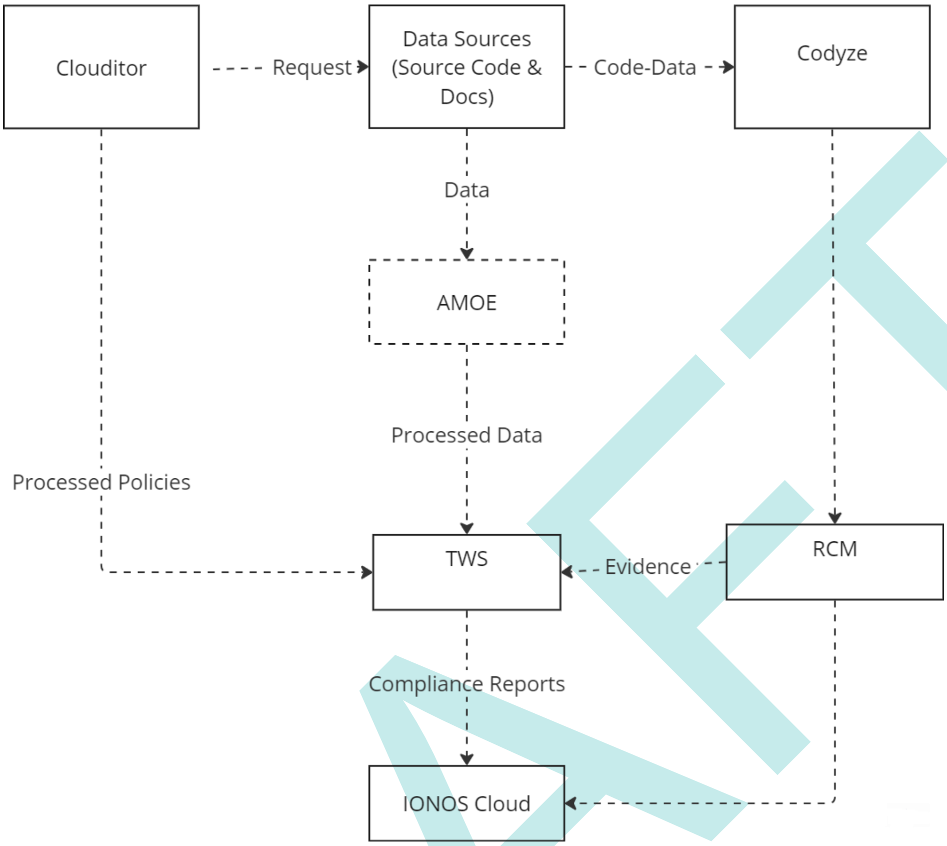


*Figure 3. Initial workflow diagram of pilot 1*

### 2.1.2.6 Business-driven Requirements

For IONOS, the primary goal of participating in pilot 1 of the EMERALD project is to establish a streamlined, effective, and continuously monitored cloud service certification process. This involvement will not only enhance security and compliance but also ensure greater customer satisfaction and trust in cloud services offered by IONOS.

Table 1 summarizes the business-driven requirements that describe the requirements of the pilot 1 towards the functionality of the EMERALD framework. The full information can be found in *APPENDIX A: Business-driven requirements*.

*Table 1. Business-driven requirements for pilot 1*

| ID | Name | Description |
|---|---|---|
| BDRP1.01 | Automate and Streamline Certification Processes | As IONOS pilot 1,<br>we want the certification process to be automated, so that the time spent on manual entries can be reduced and we focus more on strategic compliance planning. |
| BDRP1.02 | Secure and Reliable Long-term Evidence Storage | As IONOS pilot 1,<br>we need a system that securely stores all compliance evidence long-term, |

| | | |
|---|---|---|
| | | so that we can retrieve it quickly and reliably for any audits or compliance checks without fearing data loss or corruption. |
| BDRP1.03 | Efficient Requirement and Compliance Mapping | As IONOS pilot 1,<br>we want to use an AI-assisted mapping tool to quickly align our service offerings with multiple compliance frameworks, ensuring accuracy and saving time on cross-referencing standards manually. |
| BDRP1.04 | Central Management of Controls and Metrics | As IONOS pilot 1,<br>we need a central repository to easily manage and update security controls and metrics to propagate changes accurately and timely across all compliance documentation and reports. |
| BDRP1.05 | Compliance Verification for Organizational Policies | As IONOS pilot 1,<br>we want a tool that can automatically assess our organizational policies against compliance standards,<br>so that we can easily identify and address gaps in our internal policies without manually reviewing each one. |
| BDRP1.06 | Ensure Software Compliance through Static Code Analysis | As IONOS pilot 1,<br>we need a static code analysis tool that integrates into our CI/CD pipeline to verify compliance before deployment, ensuring that any compliance issues are caught and resolved early in the development process |
| BDRP1.07 | Intuitive User Experience for Compliance Monitoring | As IONOS pilot 1,<br>we want a user-friendly interface that allows us to monitor compliance status across various cloud services easily,<br>so that we can make quick decisions based on real-time data and effectively communicate compliance status to stakeholders. |

### 2.1.2.7 Pilot KPIs

The following are the KPIs defined to evaluate the success of pilot 1. They are essential for ensuring that the pilot aligns with the business objectives.

| **KPI** | **1.1- Reduction in Certification Time** |
|---|---|
| **Description** | Measure the decrease in time required to achieve and renew certifications with the EMERALD framework compared to traditional methods |
| **Goal** | Reduce certification time |
| **Priority** | High |
| **Benefit** | Faster certification processes allow quicker market entry for new services and updates, improving business agility |
| **Obstacle** | Integrating automated processes with existing manual processes may require significant initial adjustments and training |
| **Measurement** | |

| | |
|---|---|
| **Measured by** | Time taken from the start of the certification process to its completion |
| **Unit** | Days |
| **Baseline value** | Average days taken prior to the EMERALD implementation |

| **KPI** | **1.2 – Compliance Error Rate** |
|---|---|
| **Description** | Track the rate of compliance errors or omissions identified during audits |
| **Goal** | Achieve a reduction of 40% in compliance errors |
| **Priority** | High |
| **Benefit** | Enhances the reliability and security of IONOS services, ensuring adherence to regulatory standards |
| **Obstacle** | Potential resistance to new automated tools and processes, which could initially lead to errors in handling or data entry |
| **Measurement** | |
| **Measured by** | Compliance audit reports |
| **Unit** | # of errors |
| **Baseline value** | Average number of errors reported in audits prior to EMERALD |

| **KPI** | **1.3 – Audit Preparation Cost** |
|---|---|
| **Description** | Assess the financial impact of EMERALD by measuring the reduction in costs associated with preparing for audits |
| **Goal** | Reduce audit preparation costs |
| **Priority** | High |
| **Benefit** | Lower costs lead to more resources available for other strategic initiatives and improvements |
| **Obstacle** | Initial investment in the EMERALD system and potential unforeseen costs during integration |
| **Measurement** | |
| **Measured by** | Financial accounting and reporting systems |
| **Unit** | Euro (€) |
| **Baseline value** | Current average cost of audit preparation |

| **KPI** | **1.4 – User Satisfaction Score** |
|---|---|
| **Description** | Evaluate the satisfaction of internal users (compliance managers, auditors) with the new EMERALD framework |
| **Goal** | Achieve higher user satisfaction score |
| **Priority** | High |
| **Benefit** | High user satisfaction indicates effective implementation and user-friendliness of the EMERALD framework, leading to better adoption |
| **Obstacle** | Resistance to change and the learning curve associated with new systems |
| **Measurement** | |
| **Measured by** | Internal survey tools |

| | |
|---|---|
| **Unit** | Percentage |
| **Baseline value** | Satisfaction level prior to EMERALD, based on internal surveys |

| **KPI** | **1.5 – Interoperability Incident Rate** |
|---|---|
| **Description** | Track the frequency of incidents related to interoperability issues with other systems and services post-EMERALD integration |
| **Goal** | Reduce interoperability incidents |
| **Priority** | High |
| **Benefit** | Smooth interoperability enhances service reliability and customer experience |
| **Obstacle** | Compatibility issues with existing IT infrastructure or third-party services |
| **Measurement** | |
| **Measured by** | IT support incident logs |
| **Unit** | # of Incidents |
| **Baseline value** | Current rate of interoperability incidents before implementation |

### 2.1.3 Integration Approach

This section outlines the strategic and technical processes through which the EMERALD components will be seamlessly incorporated within the IONOS cloud infrastructure for pilot 1.

#### *2.1.3.1 Identification of Certification Targets*

The following tables present certification targets which can be used by the EMERALD evidence collection tools as basis for the certification of pilot 1. These targets are tentatively proposed and subject to further validation and potential modification by the security team during the pilot implementation. Depending on the evolving needs and security assessments, additional certification targets may be included in pilot 1 to ensure a comprehensive and effective compliance framework.

| **Certification Target** | **Source Code Repositories** |
|---|---|
| **Type** | Code |
| **Description** | Repositories containing all source code for cloud services |
| **Availability to component owner(s)** | Available via secure API or direct repository access with proper authentication |
| **Evidence Collection Tool** | **Codyze** |
| **Hosting** | EMERALD |
| **Evidence stored at** | IONOS Cloud/EMERALD |
| **Evidence processed at** | IONOS Cloud |
| **Processed results integrated in** | EMERALD UI/UX |

| **Certification Target** | **Organizational Policy Documents** |
|---|---|
| **Type** | Document |
| **Description** | Documents outlining organizational security policies and procedures |
| **Availability to component owner(s)** | Stored in a centralized document management system accessible to compliance managers |

| Evidence Collection Tool | AMOE |
|---|---|
| **Hosting** | EMERALD |
| **Evidence stored at** | IONOS Cloud/EMERALD |
| **Evidence processed at** | IONOS Cloud |
| **Processed results integrated in** | EMERALD UI/UX |

### *2.1.3.2 Integration and Application of Components*

The integration and application section details how specific EMERALD components like Clouditor, TWS, and MARI are deployed and utilized within pilot 1. It includes descriptions of component functionalities, integration strategies, and access controls to ensure effective and secure operations.

#### 2.1.3.2.1 Clouditor/Orchestrator

- (How) will the component be used in the pilot?
    - Clouditor will be used as the orchestration hub and will act as the central command centre for managing the compliance workflow.
- What are the expected benefits?
    - It will automate tasks such as initiating compliance checks, aggregating results from other components like Codyze for code analysis, and AMOE for policy assessment, and compiling these into compliance reports.
- What are the component-specific requirements?
    - A high-level requirement of this component at this point, is that it needs to integrate seamlessly with existing IaaS systems at IONOS and must support the automation of compliance checks for targeted certificates which are introduced above.
- Where will it be hosted (EMERALD/pilot-specific)?
    - The current plan is to host the component within the IONOS cloud infrastructure to ensure secure and reliable access during the pilot.
- Who should have access (roles/permissions) to which results of the component?
    - Compliance managers and cloud security managers at IONOS will have access to the orchestration results; IT security auditors will have read-only access for verification.

#### 2.1.3.2.2 Trustworthiness System (TWS)

- (How) will the component be used in the pilot?
    - TWS will securely store all long-term compliance and audit-related evidence. It will be integrated to receive inputs from all components, ensuring that evidence collected during compliance checks is securely logged and retrievable for future audits.
- What are the expected benefits?
    - This will facilitate a comprehensive audit trail that supports compliance verification over time.
- What are the component-specific requirements?
    - Overall, the component is required to ensure high-security storage and quick data retrieval capabilities. Compliance with GDPR and other privacy standards is essential.
- Where will it be hosted (EMERALD/pilot-specific)?
    - In a secure segment of the IONOS data centre allocated for compliance and security-sensitive operations.
- Who should have access (roles/permissions) to which results of the component?

  - IT security auditors and compliance officers of IONOS should have full access, with audit logs available to senior management for oversight.

### 2.1.3.2.3 Mapping Assistant for Requirements with Intelligence (MARI)

- (How) will the component be used in the pilot?
  - MARI will utilize artificial intelligence to efficiently map IONOS cloud service offerings against applicable compliance frameworks.
- What are the expected benefits?
- This component will draw on data from the RCM to ensure accurate alignment of metrics with compliance controls, reducing manual mapping efforts.
- What are the component-specific requirements?
  - MARI requires up-to-date datasets of compliance frameworks and the ability to learn from adjustments made by compliance officers.
- Where will it be hosted (EMERALD/pilot-specific)?
  - It will be hosted where the pilot can leverage centralized AI learning and updates.
- Who should have access (roles/permissions) to which results of the component?
  - Compliance officers primarily, with oversight access for risk managers to review and confirm alignment.

### 2.1.3.2.4 Repository of Controls and Metrics (RCM)

- (How) will the component be used in the pilot?
  - RCM will act as a centralized database for all controls, requirements, and metrics related to cloud service certifications at IONOS.
- What are the expected benefits?
  - It ensures consistency and reliability in compliance data across the organization, facilitating quicker updates and compliance checks.
- What are the component-specific requirements?
  - This component requires to support real-time updates and integration with other EMERALD components like Clouditor and RMA.
- Where will it be hosted (EMERALD/pilot-specific)?
  - The hosting environment will be selected considering the need to ensure integration with other components and centralized management.
- Who should have access (roles/permissions) to which results of the component?
  - System administrators and compliance managers will have edit access; auditors and risk managers will have read-only access.

### 2.1.3.2.5 AMOE, Codyze, AI-SEC, and EMERALD UI/UX

- (How) will the component be used in the pilot?
  - These components will handle specific tasks like assessing organizational policies (AMOE), conducting static code analysis (Codyze), evaluating AI model security (AI-SEC), and providing a user interface (EMERALD UI/UX).
- What are the expected benefits?
  - They enhance specific areas such as policy compliance, code security, AI safety, and user experience, respectively.
- What are the component-specific requirements?
  - Each component must integrate with the IONOS infrastructure and meet specific operational benchmarks like speed, accuracy, and user-friendliness.
- Where will it be hosted (EMERALD/pilot-specific)?
  - Each will be hosted within the IONOS infrastructure to maintain security and integration across the system.

- Who should have access (roles/permissions) to which results of the component?
    - Different levels of access for different roles based on their needs—developers for Codyze, AI developers for AI-SEC, compliance officers for AMOE, and various users for EMERALD.

## 2.2 Pilot 2: CloudFerro

This section introduces pilot 2 which aims at demonstrating Certification as a Service with EMERALD on IaaS / PaaS. To achieve this goal, CloudFerro will set up test environments which will be used by the EMERALD components for evidence collection. Details are described in the following sections.

### 2.2.1 Introduction and Motivation

CloudFerro (CF) provides cloud computing services dedicated to specific industries. CF specializes in the storage and processing of large data sets, including Earth observation satellite data repositories. It is the largest company in the Polish space sector, a leader in the European Earth Observation sector and a prime contractor for institutions such as ESA, EUMETSAT, ECMWF and DLR. CloudFerro as a Cloud Service Provider (CSP) is one of the main EMERALD's stakeholders and will validate project outcomes in pilot 2.

The main goal of all pilots is to validate project outcomes in real life use cases. pilot 2, as a part of Category I, is aimed at testing tools in IaaS/PaaS environment on public cloud. Therefore, in order to be able to carry out a real-life use case, CF will provide resources on its public cloud and prepare IaaS and PaaS test environments, which will be used for evidence collection by EMERALD tools.

#### *2.2.1.1 Current Practice and Problem Statement (before EMERALD)*

CloudFerro has three security audits each year – ISO 27001, BSI 200-1, BSI C5. They are all time-consuming because they are comprehensive. Audit usually takes 2-4 days, but a lot of time is also needed for preparation. Main data for audits are existing audit checklist, policies, procedures (not all must be documented), specifications, descriptions etc. Currently we do not use any tools, we do everything manually.

#### *2.2.1.2 Expected Benefits (after EMERALD)*

CloudFerro's audit right now are based on documentation and demand manual work of many people for days. Because of that, our main goals to achieve by using EMERALD are:

- Automation of document verification process
- Reduction of audit cost - decrease of time or/and people needed for audit because of EMERALD tools
- Reusability of tools - faster and easier recertification (and audits)

### 2.2.2 Pilot Definition

This section provides details of pilot 2, such as architecture, roles, workflow etc.

#### *2.2.2.1 Pilot Diagram*

Figure 4 shows three main roles in pilot 2 which will use EMERALD and the use cases for each of them.

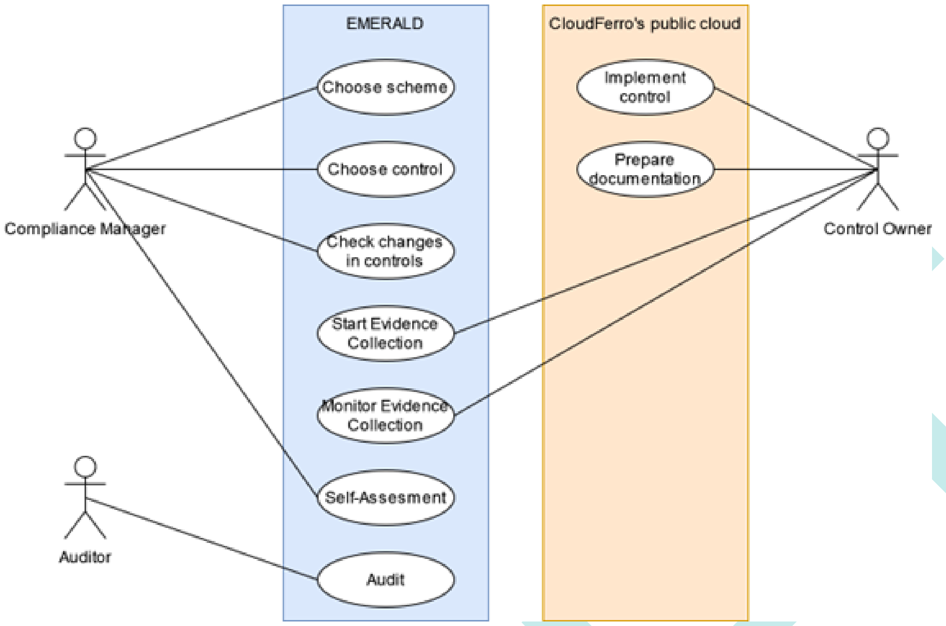


*Figure 4. Pilot 2 roles and use cases*

The two use cases "Implement control" and "Prepare documentation", although they pertain to the CF's public cloud and not to EMERALD, have been included in the diagram because they are essential steps in the pilot 2 workflow. Details of the roles are presented in Table 2.

*Table 2. Description of Pilot 2 roles*

| Role | Description |
|---|---|
| **Control Owner** | Person responsible for control implementation (in CF's clouds or by documentation preparation).<br>Depending on the control/requirement, it can be represented by product owners, security employees, compliance manager etc. |
| **Compliance Manager** | Person responsible for the whole certification process, i.e., choose scheme and verify compliance of all controls.<br>Main person involved in audits. |
| **Auditor** | Person who audits the company. In EMERALD it will be represented by NIXU. More details in Section 3.1 (Stage Gate Process). |

#### 2.2.2.2 Pilot Workflow

Pilot 2 workflow can be described in 7 general steps:

1. CF Compliance Manager chooses a certification scheme.
2. CF Compliance Manager chooses controls for implementation (in case of recertification CF Compliance Manager checks if there are any changes in requirements, controls etc.)
3. CF Control Owner implements controls in test environments (in case of organizational controls CF Control Owner prepares proper documentation).
4. CF Control Owner starts evidence collection (cloud discovery + policy documents).
5. CF Control Owner monitors evidence collection.
6. CF Compliance Manager verifies compliance. Self-Assessment is completed.
7. Auditor audits the company.

#### 2.2.2.3 Technical perspective and system architecture

Figure 5 shows a high-level architecture of Pilot 2.

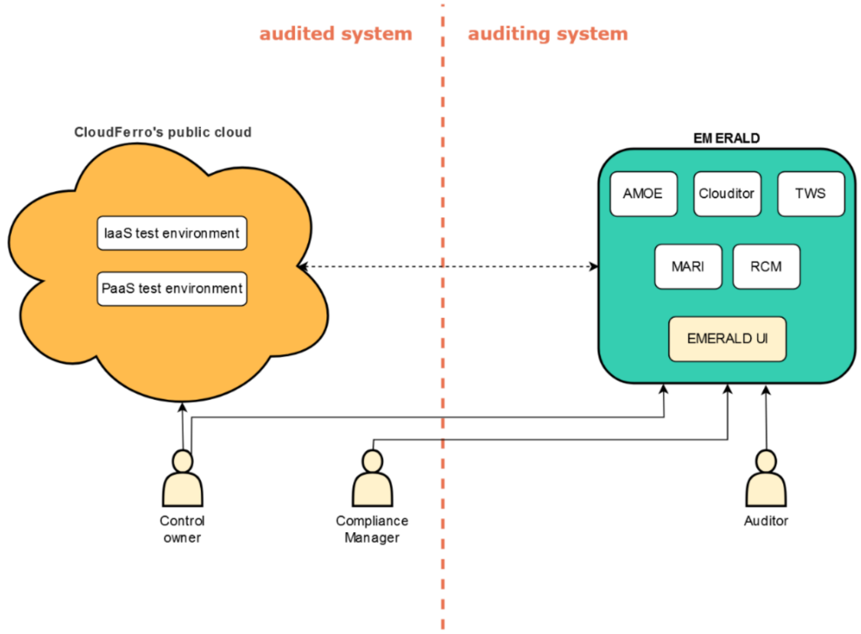


*Figure 5. Pilot 2 high level architecture*

Pilot 2 is aimed at testing tools in an IaaS/PaaS environment on public cloud. CF will provide resources on its public cloud and prepare IaaS and PaaS test environments, which will be used for evidence collection by the EMERALD tools. The **IaaS environment** will consist of computing and/or storage resources. The **PaaS environment** will be based on a container orchestration solution.

We plan to host all the EMERALD components at the EMERALD infrastructure managed by TECNALIA and not at the pilot itself. Technical requirements will be met based on evidence collected from these IaaS and PaaS environments. The evidence will be gathered by Clouditor via API. Organizational requirements will be met based on evidence collected from documentation (policies, etc.). Proper documentation will be prepared by CF employees and evidence will be gathered by AMOE. RCM (which stores certification schemes, controls, etc.) and MARI (responsible for mapping metrics to controls) will also be used in the process of meeting the security controls. At the end of this process TWS will ensure storage of evidence and assessment results. Users will interact with EMERALD and its components using the EMERALD UI.

#### 2.2.2.4 Security controls and measures

CloudFerro will prepare IaaS and PaaS dedicated test environments, which will be separated from any production environment. However, these environments will be prepared in accordance with internal security policies and procedures and access to them will be restricted, as they will be one of CF's public clouds. We do not plan to host any EMERALD components at the pilot itself, and data from evidence collection will be stored in the EMERALD infrastructure hosted by TECNALIA. Taking all of this into account, we decided not to not perform any security related testing.

### 2.2.2.5 Communication and workflow diagram

Figure 6 presents the pilot 2 workflow (from section 2.2.2.2) and the interactions between all roles (from section 2.2.2.1). First, the *Compliance Manager* chooses a certification scheme. If it is recertification, the *Compliance Manager* verifies whether there have been any changes and, if so, chooses the controls for implementation. The technical controls are then implemented and the documentation for organizational controls is prepared by the *Control Owner*, who initiates the collection of evidence and monitors the results. The *Compliance Manager* verifies compliance through a self-assessment. Once completed, the *Auditor* audits the company.

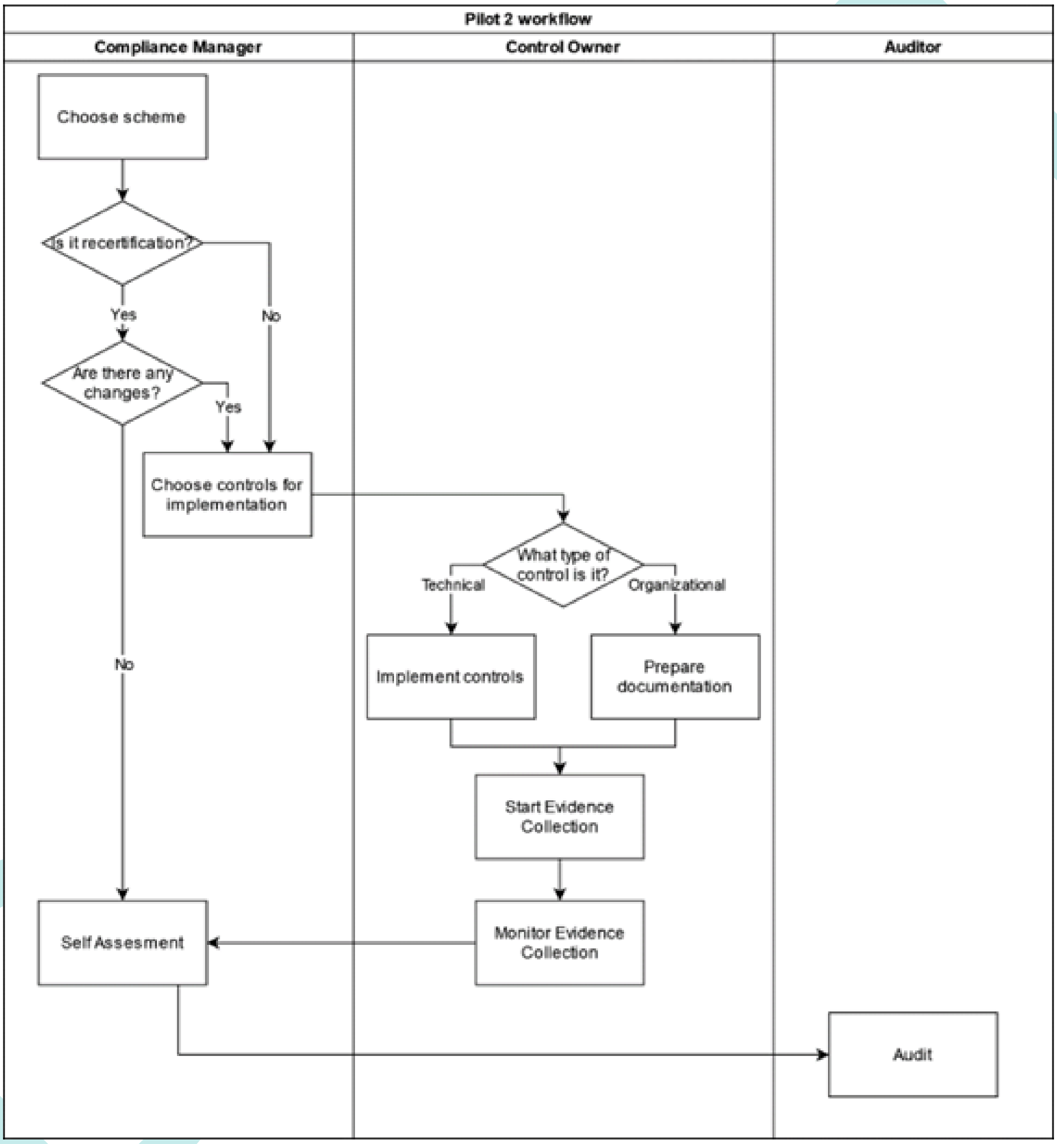


*Figure 6. Pilot 2 workflow diagram*

### 2.2.2.6 Business-driven Requirements

Table 3 summarizes the business-driven requirements that describe the requirements of the pilot2 towards the functionality of the EMERALD framework. The full information can be found in *APPENDIX A: Business-driven requirements*.

*Table 3. Business-driven requirements for pilot 2*

| ID | Name | Description |
|---|---|---|
| BDRP2.01 | OpenStack | As CloudFerro,<br>I want EMERALD to be able to gather evidence collection about resources from OpenStack (including Magnum for PaaS),<br>so that we can use it. |
| BDRP2.02 | Reusable Metrics & Requirements | As CloudFerro,<br>I want that a requirement or metric which was already implemented can be reused,<br>so that the audit time can be decreased. |
| BDRP2.03 | Transparency increase | As CloudFerro,<br>I want that EMERALD increases transparency for our clients and users about our certificates and audits,<br>so that we can ensure to our clients that our services are secured. |
| BDRP2.04 | Intuitive UI | As CloudFerro,<br>I want that EMERALD has an intuitive UI which is readable for everyone,<br>so that even non-technical employees, like compliance managers, can use it without problem. |
| BDRP2.05 | Security Schemes | As CloudFerro,<br>I want EMERALD tools to certify BSI-C5 (must), ISO 27001 (could), BSI 200-1 (could),<br>so that EMERALD can support us with certificates we already use. |

#### 2.2.2.7 Pilot KPIs

The following pilot KPIs describe the goals that pilot 2 aims to achieve using EMERALD.

| **KPI** | **2.1 – Time needed for audit** |
|---|---|
| **Description** | Time in hours needed for the whole audit (without time spent by auditors) |
| **Goal** | Decrease |
| **Priority** | 1 - must |
| **Benefit** | Reducing the time needed for audits will result in reduced audit costs, which is the main goal of our pilot and could be one of the biggest advantages of using EMERALD tools |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Estimation time |
| **Measurement Interval** | Begin & end of project |
| **Unit** | h |
| **Baseline value** | Not available |

| **KPI** | **2.2 – Cost for audit** |
|---|---|
| **Description** | Cost of employees involved in the audit process (without time spent by auditors) |
| **Goal** | Decrease |
| **Priority** | 1 - must |
| **Benefit** | Decrease of time needed for audit will result in decrease of audits cost what is main goal in our pilot and could be one of the biggest advantages of using EMERALD tools |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Estimation time*hourly rate |
| **Measurement Interval** | Begin & end of project |
| **Unit** | € |
| **Baseline value** | Not available |

| **KPI** | **2.3 – Employees needed for audit** |
|---|---|
| **Description** | Number of employees involved in an audit process (without auditors) |
| **Goal** | Decrease |
| **Priority** | 2 - should |
| **Benefit** | Reducing the number of employees needed for audits will result in lower audits cost, which is main goal in our pilot and could be one of the biggest advantages of using EMERALD tools |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Estimated number of employees involved in audit process |
| **Measurement Interval** | Begin & end of project |
| **Unit** | int |
| **Baseline value** | Not available |

| **KPI** | **2.4 – Time needed for audit preparation** |
|---|---|
| **Description** | Time in hours needed for all audit preparation activities, for example documentation verification (without time spent by auditors) |
| **Goal** | Decrease |
| **Priority** | 1 - must |
| **Benefit** | Reducing the time needed for audit preparation will result in lower audits cost, which is the main goal in our pilot and could be one of the biggest advantages of using EMERALD tools |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Estimation time |
| **Measurement Interval** | Begin & end of project |
| **Unit** | h |

| | |
|---|---|
| **Baseline value** | Not available |

| **KPI** | **2.5 – Time needed to meet a requirement** |
|---|---|
| **Description** | Time in hours/minutes from evidence collector discovery, through mapping metrics to meet a requirement |
| **Goal** | Decrease (shorter than manual) |
| **Priority** | 2 - should |
| **Benefit** | Achieving this goal means that we can meet requirements faster/automatically with EMERALD tools, so in the context of pilot2 it shows that using these tools makes sense and makes manual work easier and faster. |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | End time - start time |
| **Measurement Interval** | Begin & end of project |
| **Unit** | h/min |
| **Baseline value** | Not available |

| **KPI** | **2.6 – Time needed to meet a requirement again** |
|---|---|
| **Description** | Time in hours/minutes needed to meet a requirement which has been already implemented |
| **Goal** | Decrease (shorter than 2.5) |
| **Priority** | 1 - must |
| **Benefit** | Achieving this goal means that the tools are reusable, and they make recertification/reaudit faster and easier. |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | End time - start time |
| **Measurement Interval** | End of project |
| **Unit** | h/min |
| **Baseline value** | Not available |

| **KPI** | **2.7 – Coverage of scheme** |
|---|---|
| **Description** | How many requirements of a scheme can be covered (automated) by EMERALD tools |
| **Goal** | 80% (of chosen sample) |
| **Priority** | 2 - should |
| **Benefit** | Achieving this goal shows that using EMERALD tools makes sense, because they help us automate our work |
| **Obstacle** | Currently CF doesn't use any automation tools, so in any case it will be an increase. That's why we chose a specific value to achieve. |
| **Measurement** | |

| | |
|---|---|
| **Measured by** | Number of covered requirements/numbers all of requirements |
| **Measurement Interval** | End of project |
| **Unit** | % |
| **Baseline value** | 0% |

| **KPI** | **2.8 – Time needed for document verification** |
|---|---|
| **Description** | Time in hours needed for the document verification process |
| **Goal** | Decrease (shorter than manual) |
| **Priority** | 1 - must |
| **Benefit** | Achieving this goal shows that using EMERALD tools makes sense, because they help us automate our work |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Estimation time |
| **Measurement Interval** | Begin & end of project |
| **Unit** | h |
| **Baseline value** | Not available |

| **KPI** | **2.9 – Possibility to use tools for different cloud service models** |
|---|---|
| **Description** | Checking whether it is possible to meet the proper requirements for different cloud service models. |
| **Goal** | Ability to use EMERALD for IaaS and PaaS |
| **Priority** | 1 - must |
| **Benefit** | Achieving this goal is necessary to conduct the pilot according to its definition - IaaS/PaaS on public clouds. |
| **Obstacle** | No obstacle identified |
| **Measurement** | |
| **Measured by** | Provided by the user after verifying whether it is possible to meet the requirements for IaaS and PaaS |
| **Measurement Interval** | End of project |
| **Unit** | Boolean |
| **Baseline value** | No |

### 2.2.3 Integration Approach

This section describes how the pilot 2 will integrate EMERALD components into its systems.

#### *2.2.3.1 Identification of Certification Targets*

The following tables present which targets should be certified by EMERALD in pilot 2.

| **Certification Target** | **IaaS environment** |
|---|---|
| **Type** | Service |

| | |
|---|---|
| **Description** | Test IaaS environment will be based on CF's public cloud with resources like VMs, Storage etc. |
| **Availability to component owner(s)** | CF employees will have access to the IaaS environment. The evidence gathered from the environment via API will be available in EMERALD. |
| **Evidence Collection Tool** | **Clouditor** |
| **Hosting** | EMERALD |
| **Evidence stored at** | Evidence gathered from the environment via API can be stored in EMERALD. |
| **Evidence processed at** | Evidence gathered from the environment via API can be processed in EMERALD. |
| **Processed results integrated in** | Results will be used in the TWS, EMERALD UI and in any other components if needed. |

| **Certification Target** | **PaaS environment** |
|---|---|
| **Type** | Service |
| **Description** | Test PaaS environment will be based on container orchestration solution. |
| **Availability to component owner(s)** | CF employees will have access to the PaaS environment. The evidence gathered from the environment via API will be available in EMERALD. |
| **Evidence Collection Tool** | **Clouditor** |
| **Hosting** | EMERALD |
| **Evidence stored at** | Evidence gathered from the environment via API can be stored in EMERALD. |
| **Evidence processed at** | Evidence gathered from the environment via API can be processed in EMERALD. |
| **Processed results integrated in** | Results will be used in TWS, EMERALD UI and in any other components if needed. |

| **Certification Target** | **Policy** |
|---|---|
| **Type** | Document |
| **Description** | All anonymized documentation which is needed to gather evidence. |
| **Availability to component owner(s)** | Documentation in anonymized version (without private company details) could be shared. |
| **Evidence Collection Tool** | **AMOE** |
| **Hosting** | EMERALD |
| **Evidence stored at** | Evidence gathered from the environment via API can be stored in EMERALD. |
| **Evidence processed at** | Evidence gathered from the environment via API can be processed in EMERALD. |
| **Processed results integrated in** | Results will be used in TWS, EMERALD UI and in any other components if needed. |

### 2.2.3.2 Integration and Application of Components

CF plans to host all EMERALD components at the EMERALD infrastructure hosted by TECNALIA, and not at the pilot itself.

#### 2.2.3.2.1 Clouditor/Orchestrator

- (How) will the component be used in the pilot?
    - Clouditor will be used for cloud resources evidence collection.
- What are the expected benefits?
    - Automatic compliance for technical requirements.
- What are the component-specific requirements?
    - Clouditor must be able to gather evidence from cloud based on OpenStack (BDRP2.01).
- Who should have access (roles/permissions) to which results of the component?
    - Control Owner – set-up, monitor and manage discovery process.
    - Compliance Manager - set-up, monitor and manage discovery process.
    - Auditor – monitor results.

#### 2.2.3.2.2 Trustworthiness System (TWS)

- (How) will the component be used in the pilot?
- TWS will be used as storage of hashes of evidence and assessment results.
- What are the expected benefits?
    - Increase of transparency.
- What are the component-specific requirements?
    - There are no pilot specific requirements.
- Who should have access (roles/permissions) to which results of the component?
    - Compliance Manager and Auditor should have access to evidence and assessment result.

#### 2.2.3.2.3 Mapping Assistant for Requirements with Intelligence (MARI)

- (How) will the component be used in the pilot?
    - MARI will be used to map metrics to controls/requirements.
- What are the expected benefits?
    - Automatic mapping of metrics to controls/requirements.
- What are the component-specific requirements?
    - There are no pilot specific requirements.
- Who should have access (roles/permissions) to which results of the component?
    - Compliance Manager and Control Owner should have access to mapping results.

#### 2.2.3.2.4 Repository of Controls and Metrics (RCM)

- (How) will the component be used in the pilot?
    - RCM will be used as a storage of certification schemes and relevant controls.
- What are the expected benefits?
    - Easy access to controls of a chosen certification scheme.
- What are the component-specific requirements?
    - BSI-C5 available in RCM (BDRP2.05).
- Who should have access (roles/permissions) to which results of the component?
    - Compliance Manager should have access to the list of all certification schemes, controls, etc.
    - Control Owner should have access only to relevant controls.

#### 2.2.3.2.5 AMOE

- (How) will the component be used in the pilot?
    - AMOE will be used to get evidence collection from documentation like policies etc.
- What are the expected benefits?
    - Automation of the document verification process.
- What are the component-specific requirements?
    - There are no pilot specific requirements.
- Who should have access (roles/permissions) to which results of the component?
    - Compliance Manager and Control Owner should have access to evidence results.

#### 2.2.3.2.6 Codyze, eknows, AI-SEC

- (How) will the component be used in the pilot?
    - Codyze, eknows and AI-SEC won't be used in pilot 2.

#### 2.2.3.2.7 EMERALD UI

- (How) will the component be used in the pilot?
    - EMERALD UI will be used by users to interact with components.
- What are the expected benefits?
    - Users can interact with components and have access only to those they should.
- What are the component-specific requirements?
    - It should be intuitive and readable even for non-technical employees (BDRP2.04).
- Who should have access (roles/permissions) to which results of the component?
    - All of users should have access to UI.

## 2.3 Pilot 3: Fabasoft

In the following section, pilot 3 is introduced, following the overall pilot structure. The pilot attempts to integrate all EMERALD tools. The goal is to achieve an assisted certification with the EUCS level high requirements and to evaluate the applicability of the pilot findings to a BSI C5 audit. For this, the Fabasoft pilot will set up a test environment which can be certified by EMERALD's CaaS approach.

### 2.3.1 Introduction and Motivation

Fabasoft PROCECO[4] is a unique business ecosystem providing selected, powerful and seamlessly integrated solutions for document-intensive business processes. The technological basis of the ecosystem is the highly secure and certified Fabasoft Cloud[5]. Fabasoft strives to be at the forefront of data protection and information security, continuously strengthening the cyber-resiliency of its products and services and providing proof of this with internationally recognized certifications.

For pilot 3, Fabasoft's traditional audits will be adapted to a continuous certification process. It is the Fabasoft pilot's intention to have defined processes which allow a fully digitalized and automated audit. The audit transparency should be further increased so that customers can easily confirm its significance.

#### *2.3.1.1 Current Practice and Problem Statement (before EMERALD)*

While continuous certification currently imposes several challenges, evidence collection and evidence processing can be fully automated by utilizing existing tools. These can be reused as basis for the Fabasoft pilot, with the goal of eventually creating a fully automated audit process.

Additionally, the Fabasoft pilot is looking to reduce the overall effort required during the certification process. This is mostly based on time consuming repetitive tasks, which require the manual work of specially trained personnel and the management of all involved personnel. As a consequence, the Fabasoft pilot seeks for a reusable set of processes and certification objects (e.g., metrics, controls) and wishes to reuse existing tooling so that established processes can be integrated.

#### *2.3.1.2 Expected Benefits (after EMERALD)*

By utilizing EMERALD and therefore adopting continuous certification in Fabasoft's audit lifecycle, the pilot seeks for higher transparency in the entire audit process, easy-to-use tooling to facilitate compliance managers' needs, reduction of manual tasks to a minimum and the creation of a centralized, enterprise-wide view for the entirety of Fabasoft's audits and its sub-processes.

### 2.3.2 Pilot definition

The Fabasoft pilot is set up to abstract the audit processes at Fabasoft which are relevant for the EMERALD project. Details regarding this are presented in this section.

#### *2.3.2.1 Pilot Diagram*

This stakeholder diagram (see Figure 7) lists all participants needed by pilot 3 and its validation phase. While stakeholders found in layer 2 will use EMERALD and its components directly, stakeholders from layer 3 and layer 4 will either benefit from the use of EMERALD or indirectly

[4] https://www.fabasoft.com/de/on-proceco

[5] https://en.wikipedia.org/wiki/Fabasoft_Folio_Cloud

use EMERALD components. EMERALD components that are not specifically created by Fabasoft for this pilot are not listed as they are part of the “EMERALD pilot 3” layer.

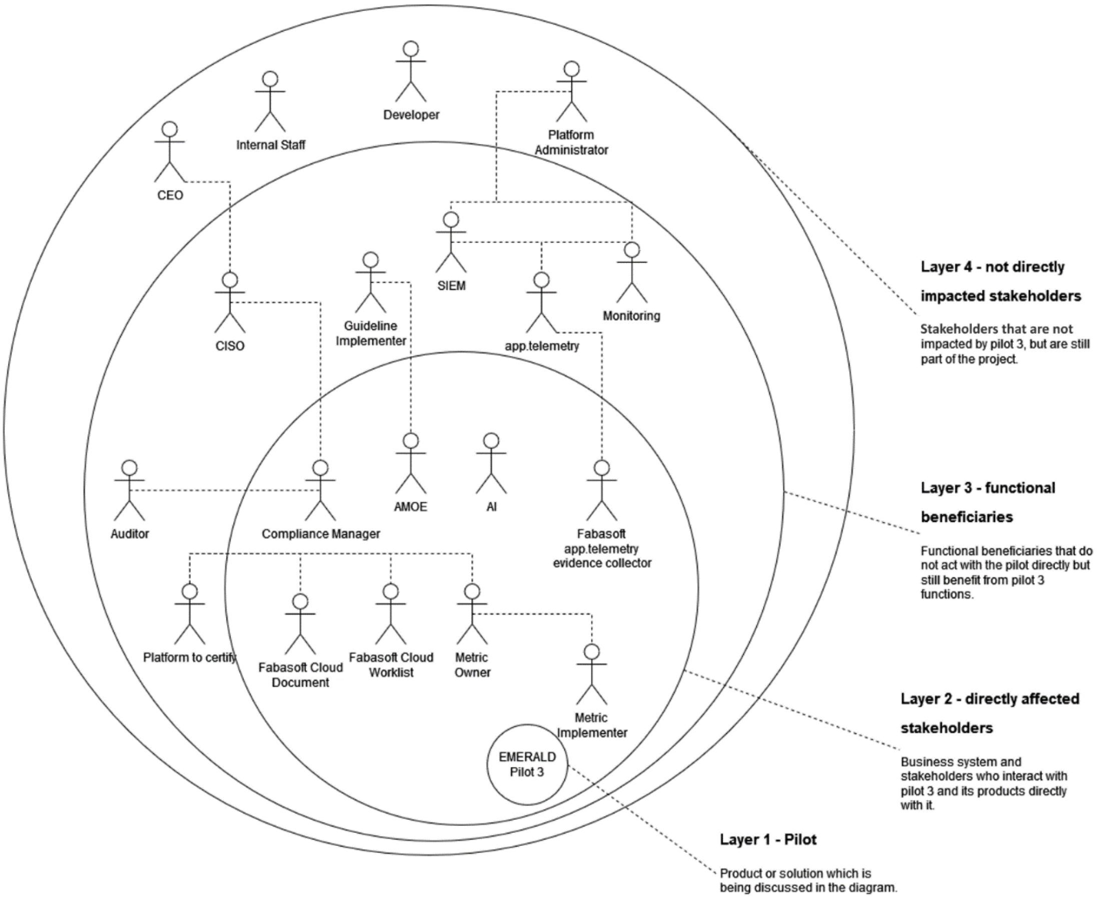

Developer
Internal Staff
Platform Administrator
CEO
SIEM
Guideline Implementer
Monitoring
CISO
app.telemetry
Layer 4 - not directly impacted stakeholders
Stakeholders that are not impacted by pilot 3, but are still part of the project.
AMOE
AI
Auditor
Compliance Manager
Fabasoft app.telemetry evidence collector
Layer 3 - functional beneficiaries
Functional beneficiaries that do not act with the pilot directly but still benefit from pilot 3 functions.
Platform to certify
Fabasoft Cloud Document
Fabasoft Cloud Worklist
Metric Owner
Metric Implementer
EMERALD Pilot 3
Layer 2 - directly affected stakeholders
Business system and stakeholders who interact with pilot 3 and its products directly with it.
Layer 1 - Pilot
Product or solution which is being discussed in the diagram.

*Figure 7. Onion Diagram of pilot 3 Stakeholders*

#### 2.3.2.2 Pilot Workflow

Pilot 3 aims for EMERALD to support all internal audit processes and to increase transparency for cloud customers. Figure 8 describes how the pilot currently perceives the application of the EMERALD framework within the EMERALD project (left) and within the pilot itself (right). The roles within the pilot were generalized for easier communication and can be adapted to the UI/UX strategy of WP4.

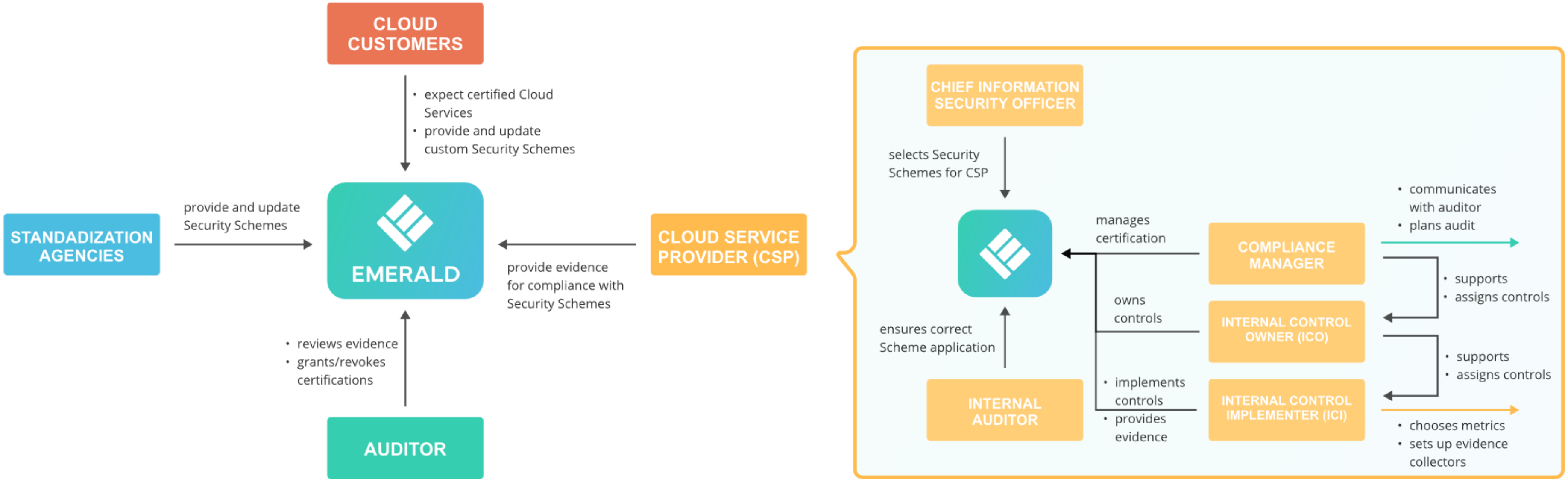

CLOUD CUSTOMERS
• expect certified Cloud Services
• provide and update custom Security Schemes
STANDADIZATION AGENCIES
provide and update Security Schemes
EMERALD
provide evidence for compliance with Security Schemes
CLOUD SERVICE PROVIDER (CSP)
• reviews evidence
• grants/revokes certifications
AUDITOR
CHIEF INFORMATION SECURITY OFFICER
selects Security Schemes for CSP
manages certification
COMPLIANCE MANAGER
• communicates with auditor
• plans audit
owns controls
INTERNAL CONTROL OWNER (ICO)
• supports
• assigns controls
ensures correct Scheme application
INTERNAL AUDITOR
• implements controls
• provides evidence
INTERNAL CONTROL IMPLEMENTER (ICI)
• supports
• assigns controls
• chooses metrics
• sets up evidence collectors

*Figure 8. Pilot 3 Workflow*

#### 2.3.2.3 Technical perspective and system architecture

The environment on which Fabasoft is going to operate and test pilot 3 is called the Fabasoft Research Platform. The pilot 3 evidence collectors will be deployed in a mix of the EMERALD environment hosted by TECNALIA and the Fabasoft Research Platform. The Fabasoft Research Platform consists among other system relevant applications (e.g., identity providers), a Kubernetes cluster setup where selected EMERALD services can be deployed and tested. Custom evidence collectors, such as described in 2.3.3 Integration Approach can be hosted there. The services will be monitored and maintained by dedicated systems which are part of the Fabasoft Research Platform.

The Fabasoft Research Platform operates on a need-to-know principle. This means that application rights are assigned when requested and are regularly revoked. For this system, CIS benchmarking[6] is implemented and selected requirements will be mapped to controls and metrics, such that the system can be integrated into the EMERALD framework.

#### 2.3.2.4 Security controls and measures

Fabasoft has created a dedicated environment for pilot 3 in which the EMERALD framework and its associated applications will be hosted. This testing environment is separated from any production environment and hosts neither security critical nor business critical applications. While the components used for this testing environment must address internal security- and organizational policies, the pilot has decided not to perform any security related testing (e.g., Pen-testing) in this context. Access to and from this environment is heavily restricted and controlled by various rules and access control lists. Furthermore, it is also possible to restrict access rights to specific EMERALD project roles within the department, if deemed necessary.

#### 2.3.2.5 Communication and workflow diagram

These diagrams (see Figure 9 and Figure 10) show the communication flow between the evidence collectors and the various components needed to put evidence into the evidence collectors.

The Cloud Evidence Collector takes a configuration, which lists all documents and properties that are needed for the evidence. After the evidence collector is configured properly, it will retrieve the data from the Fabasoft Cloud API and extract the necessary data. Once the extraction is successful, it will send the evidence to the Evidence Store, so that EMERALD can use them in the certification process.

[6] https://www.cisecurity.org/cis-benchmarks-overview

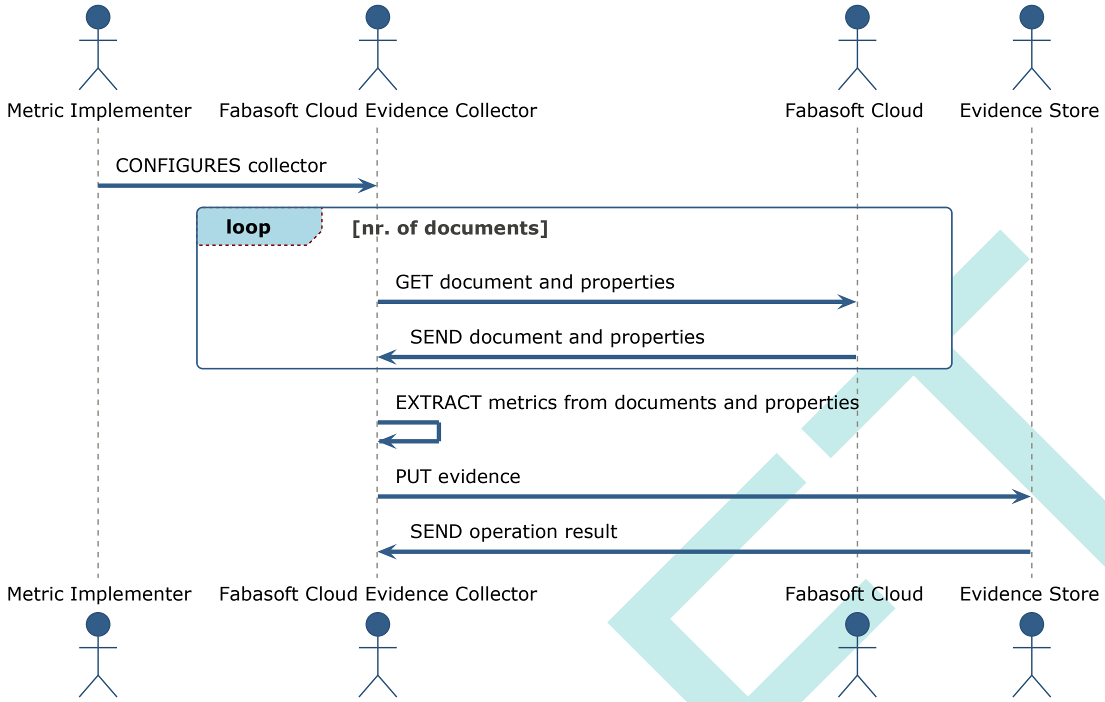

Metric Implementer
Fabasoft Cloud Evidence Collector
Fabasoft Cloud
Evidence Store
CONFIGURES collector
loop
[nr. of documents]
GET document and properties
SEND document and properties
EXTRACT metrics from documents and properties
PUT evidence
SEND operation result

*Figure 9. Document gathering flow*

While the Fabasoft app.telemetry collector serves a similar purpose to the cloud collector, instead of using the Fabasoft Cloud API it uses the Fabasoft app.telemetry API to receive the necessary system and platform metrics configured by the Metric implementer. These metrics will then be sent as evidence to the EMERALD Evidence Store.

Other collectors (e.g., Codyze) and their workflows will work as defined by the responsible partner.

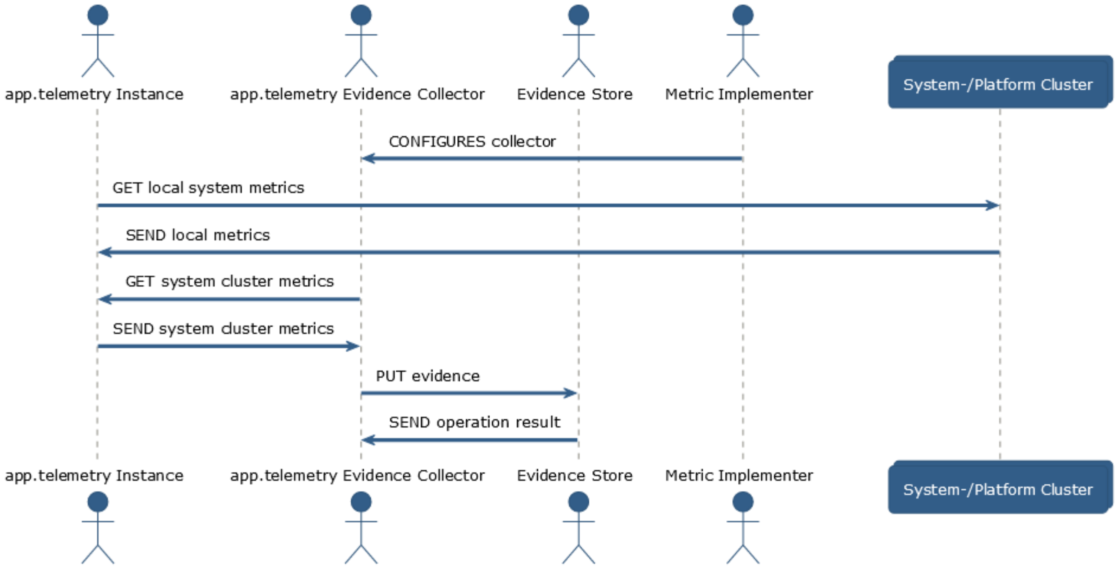


*Figure 10. Fabasoft app.telemetry flow*

### 2.3.2.6 Business-driven Requirements

Table 4 summarizes the business-driven requirements that describe the requirements of the Fabasoft pilot towards the functionality of the EMERALD framework. The full information can be found in *APPENDIX A: Business-driven requirements*.

*Table 4. Business-driven requirements for pilot 3*

| ID | Name | Description |
|---|---|---|
| BDRP3.01 | UI/UX Concept | As Fabasoft pilot 3,<br>we want a well-crafted UI/UX concept,<br>so that our users perceive EMERALD as an intuitive audit solution. |
| BDRP3.02 | AI Guideline | As Fabasoft pilot 3,<br>we want to be educated on areas of application for AI in certification-as-a-service environments with the help of EMERALD's well-structured AI guidelines,<br>so that we can reproduce this in future use cases. |
| BDRP3.03 | Integration of Internal evidence collection tools | As Fabasoft pilot 3,<br>we want to integrate our internal evidence collection tools (e.g., Fabasoft app.telemetry),<br>so that we can use and reuse the extracted evidence in the CaaS and exploit the opportunity to have our tool as a valid evidence extractor. |
| BDRP3.04 | Reusable Metrics | As Fabasoft pilot 3,<br>we want to use EMERALD's reusable metrics,<br>so that the audit process is simplified. |
| BDRP3.05 | Security Schemes pilot 3 | As Fabasoft pilot 3,<br>we want to manage Fabasoft's audit (BSI C5 (must), EUCS (must), AIC4 (must)) through the application of EMERALD,<br>so that resource consumption is minimized. |
| BDRP3.06 | Custom set of requirements | As Fabasoft pilot 3,<br>we want to manage an audit process based on an individual set of requirements – e.g., originating from a cloud customer as planned in pilot 4,<br>so that Fabasoft is able to address specific cloud customer needs as seen in the financial sector. |
| BDRP3.07 | Enhance current audit process | As Fabasoft pilot 3,<br>we want to understand how we could transfer our current audit process to EMERALD and enhance them by this change,<br>so that we understand the benefits of EMERALD and estimate any efficiency increase. |
| BDRP3.08 | Audit Transparency | As Fabasoft pilot 3,<br>we want to utilize EMERALD functionality,<br>so that the audit transparency is increased. |
| BDRP3.09 | Manual Controls | As Fabasoft,<br>we want EMERALD to have a strategy on how manual controls can be included in an automated audit (e.g., in the UI), |

| | | |
|---|---|---|
| | | so that a complete audit can be supported by EMERALD. |
| BDRP3.10 | Safe security scheme updates | As Fabasoft pilot 3,<br>we want to be aware if there is a relevant update in a security scheme we use and we want to be able to safely transfer to the new version,<br>so that we do not lose our certification or my data when we choose to update the scheme. |
| BDRP3.11 | Checks for policy documents | As Fabasoft pilot 3,<br>we would like to see if the policy document is containing the relevant information according to the requirements,<br>so that we can be sure all organizational requirements are covered, and we do not have to search the document manually. |
| BDRP3.12 | Use of standard for export/import | As Fabasoft pilot 3,<br>we want to be able to use a known standard for the export and import of information from and to the EMERALD framework,<br>so that this is easily possible where needed. |

#### 2.3.2.7 Pilot KPIs

The following pilot KPIs describe the focus of the Fabasoft pilot towards the validation of the EMERALD framework.

| **KPI** | **3.1 – Involved person per audit session** |
|---|---|
| **Description** | Number of persons required per audit session |
| **Goal** | Decrease |
| **Priority** | should |
| **Benefit** | Resource savings within organization |
| **Obstacle** | no obstacle identified |
| **Measurement** | |
| **Measured by** | Estimations of the number of persons involved in the audit process |
| **Unit** | # of persons |
| **Baseline value** | [internal] |

| **KPI** | **3.2 – Audit preparation time** |
|---|---|
| **Description** | Time in hours before the audit starts to gather all the necessary information |
| **Goal** | Decrease |
| **Priority** | should |
| **Benefit** | Time savings within organization |
| **Obstacle** | no obstacle identified |
| **Measurement** | |
| **Measured by** | Estimation by persons involved in the audit process |
| **Unit** | h |
| **Baseline value** | [internal] |

| **KPI** | **3.3 – Time to access evidence for a specific requirement** |
|---|---|
| **Description** | Time in hours needed to retrieve and assess a specific requirement and the linked evidence |
| **Goal** | Decrease |
| **Priority** | should |
| **Benefit** | Time savings within organization, better UX for employees |
| **Obstacle** | no obstacle identified |
| **Measurement** | |
| **Measured by** | User test |
| **Unit** | h |
| **Baseline value** | [internal] |

| **KPI** | **3.4 – Measuring interval** |
|---|---|
| **Description** | How often is evidence gathered and prepared for assessment |
| **Goal** | Increase |
| **Priority** | should |
| **Benefit** | As more measurements are available, the status of the certificate renews more often. |
| **Obstacle** | Arbitrary - interval could be up to the settings |
| **Measurement** | |
| **Measured by** | Review of relevant EMERALD components |
| **Unit** | Evidence collection interval (time units) |
| **Baseline value** | [internal] |

| **KPI** | **3.5 – Certificate change interval** |
|---|---|
| **Description** | How often is a new certificate issued based on the gathered evidence? |
| **Goal** | Increase |
| **Priority** | should |
| **Benefit** | Certificates portrait the actual environment and its changes better if they are updated as needed. |
| **Obstacle** | Arbitrary - interval could be up to the settings |
| **Measurement** | |
| **Measured by** | Review of relevant EMERALD components |
| **Unit** | Certificate change interval (time units) |
| **Baseline value** | [internal] |

| KPI | 3.6 – Hardware/Computing resources needed |
|---|---|
| Description | Measures how many resources are needed to reach certification with EMERALD |
| Goal | Under threshold |
| Priority | should |
| Benefit | Resources needed for audits should be reduced to increase the benefits of EMERALD |
| Obstacle | Unit dependent on resource, threshold dependent on project results |
| Measurement | |
| Measured by | Statement by EMERALD component owners |
| Unit | Unit can vary, depending on resource type |
| Baseline value | Not relevant for this KPI |

### 2.3.3 Integration Approach

This section describes how the pilot 3 plans to integrate the EMERALD components. For this, the certification targets are first introduced. Afterwards, the planned integration and application of components is presented.

#### *2.3.3.1 Identification of Certification Targets*

The following tables define an initial list of certification targets which can be used by the EMERALD evidence collection tools as basis for the certification of pilot 3. The list of certification targets is expected to be updated to the needs of the project.

| Certification Target | Policy Documents |
|---|---|
| Type | Document |
| Description | Anonymized documentation used to gather evidence for the certification by EMERALD |
| Availability to component owner(s) | Anonymized documentation will be shared |
| Evidence Collection Tool | AMOE |
| Hosting | EMERALD or pilot, depending on component requirements |
| Evidence stored at | EMERALD or pilot, depending on component requirements |
| Evidence processed at | EMERALD |
| Processed results integrated in | Any component where the processed evidence is needed |

| **Certification Target** | **Source Code Repositories** |
|---|---|
| **Type** | Code |
| **Description** | Repositories containing source code from pilot set-up. |
| **Availability to component owner(s)** | Fabasoft will have control over the code and repositories. Gathered evidence will be collected by the evidence collection tools and forwarded to the EMERALD Evidence Store component. |
| **Evidence Collection Tool** | **Codyze, eknows** |
| **Hosting** | EMERALD or pilot, depending on component requirements |
| **Evidence stored at** | EMERALD or pilot, depending on component requirements |
| **Evidence processed at** | EMERALD |
| **Processed results integrated in** | Any component where the processed evidence is needed |

| **Certification Target** | **AI Model** |
|---|---|
| **Type** | As needed |
| **Description** | Depending on the requirements of the component, a test case can be set up. |
| **Availability to component owner(s)** | Fabasoft will have control over the code and repositories. Gathered evidence will be collected by the evidence collection tools and forwarded to the EMERALD Evidence Store component. |
| **Evidence Collection Tool** | **AI-SEC** |
| **Hosting** | EMERALD or pilot, depending on component requirements |
| **Evidence stored at** | EMERALD or pilot, depending on component requirements |
| **Evidence processed at** | EMERALD |
| **Processed results integrated in** | Any component where the processed evidence is needed |

| **Certification Target** | **Fabasoft Research Platform** |
|---|---|
| **Type** | Cloud Platform |
| **Description** | See Section 2.3.2.3 |
| **Availability to component owner(s)** | Fabasoft will have control over the platform and all its tools. Gathered evidence can be collected by the evidence collection tools and forwarded to the EMERALD Evidence Store component. |
| **Evidence Collection Tool** | **Clouditor-Discovery** |
| **Hosting** | EMERALD or pilot, depending on component requirements |
| **Evidence stored at** | EMERALD or pilot, depending on component requirements |
| **Evidence processed at** | EMERALD |
| **Processed results integrated in** | Any component where the processed evidence is needed |

### *2.3.3.2 Integration and Application of Components*

With the available knowledge about the individual components at this point, the Fabasoft pilot plans to host all EMERALD components at the EMERALD infrastructure hosted by TECNALIA and not at the pilot itself. If this is not possible or beneficial for certain components, this will be discussed with the component owners. The evidence extraction tools will be deployed in the Fabasoft pilot's sandbox.

#### 2.3.3.2.1 Clouditor/Orchestrator

- How will the component be used in the pilot?
  - Clouditor will be used to check the Fabasoft pilot's Azure Realm in regard to various Security- and Transparency-Policies. At this time, the services to certify are not yet identified.
- What are the expected benefits?
  - The expected benefit of using the Clouditor/Orchestrator is that the Azure Realm pilots can be easily integrated into the certification-as-a-service process.
- What are the component-specific requirements?
  - At this point, there are no pilot specific requirements towards the Clouditor/Orchestrator, as the pilot is not yet ready to decide on this. The component owner will be informed as soon as any requirements are defined, in which case we will discuss these requirements to satisfy the needs of both parties.
- Who should have access (roles/permissions) to which results of the component?
  - The roles and permissions for the result of the components are as follows: a Compliance Manager and CISO should have access to the evidence that Clouditor provides. A metric owner/implementer should have access to evidence of metrics and controls that are assigned to them.

#### 2.3.3.2.2 Trustworthiness System (TWS)

- How will the component be used in the pilot?
  - The Trustworthiness System will be used to allow a more transparent certification process.
- What are the expected benefits?
  - By storing secure hashes of evidence provided by the various components, non-repudiation and partial-authenticity can be guaranteed. By storing a tamper-proof record that allows to verify the authenticity of evidence stored in the EMERALD Framework, it allows auditors to verify evidence without fearing tampered data. This makes the entire EMERALD Framework more reliable for any involved personnel.
- What are the component-specific requirements?
  - The results of the TWS should be easily visible and understandable in the EMERALD UI for both auditors as well as any personnel at the CSP with the respective permissions. It has to be immediately clear for these roles if the evidence is verified and whether it was tempered with.
- Who should have access (roles/permissions) to which results of the component?
  - A compliance manager and a CISO from the CSP should have access to the information from the TWS. This also applies to the auditors of the CSP.

#### 2.3.3.2.3 Mapping Assistant for Requirements with Intelligence (MARI)

- How will the component be used in the pilot?
  - MARI will be used to map controls from various security schemes to each other and to metrics which are suited for providing the necessary evidence.
- What are the expected benefits?
  - The pilot expects that MARI will enable a CSP to save valuable resources by increasing the speed and reducing the effort re-quired to map security controls

from different schemes. If a similar control is already implemented, it can be easily found and matched. This will reduce repetitive work.

- What are the component-specific requirements?
  - The MARI tool should be integrated seamlessly into the EMERALD UI. It should make it easily visible via the EMERALD UI, if a control or metric already has been implemented for a different security scheme at the pilot. It should then be possible to apply the implementation to the new control, so time can be saved, and mistakes can be avoided.
- Who should have access (roles/permissions) to which results of the component?
  - This information should be available to internal control implementers which are assigned to the respective controls.

#### 2.3.3.2.4 Repository of Controls and Metrics (RCM)

- How will the component be used in the pilot?
  - The Repository of controls and metrics contains the security schemes available in EMERALD and other relevant information.
- What are the expected benefits?
  - This can save time for the pilot, as the schemes can be used as required.
- What are the component-specific requirements?
  - Pilot 3 would like to be able to access the full information about a security scheme, even if not all controls can be continuously and automatically certified, so that the pilot is able to also manage manual controls via EMERALD in the EMERALD UI.
- Who should have access (roles/permissions) to which results of the component?
  - Pilot specific information should only be accessible by pilot specific roles, or auditors which are working with the pilot, if the information is required.

#### 2.3.3.2.5 AMOE

- How will the component be used in the pilot?
  - AMOE will be used in the pilot as evidence gathering tool for policy documents. Relevant security controls and metrics still have to be identified. As a result, the required policy documents are not yet known.
- What are the expected benefits?
  - Pilot 3 expects that AMOE can not only support the users by gathering evidence from policy documents, but can furthermore support them by quickly locating where the evidence can be found in the documents. This can be helpful for reviews of the implementation of a metric. It could also support auditors in their work, as it allows to find contradictory information in documents provided as evidence for a metric.
- What are the component-specific requirements?
  - AMOE should be integrated seamlessly into the EMERALD UI. It should be possible for a user to select the correct evidence(s) for a metric. It should be possible to apply an uploaded policy document to several security schemes. The uploaded documents need to be managed at a central point, where they can also be deleted again. The user has to be able to see which document is used as evidence for which metrics. There should be a workflow for updating or exchanging documents without immediately losing the certification. The policy documents and raw evidence should not be available outside of the pilot unless access was granted by the compliance manager.
- Who should have access (roles/permissions) to which results of the component?

  - A compliance manager and a CISO should have access (read/write/delete) to all information about the pilot from AMOE. An internal control owner and internal control implementer should have this access while a control is assigned to them. Only Compliance Managers and CISOs can delete documents.

#### 2.3.3.2.6 Codyze & eknows

- How will the component be used in the pilot?
  - Both Codyze and eknows will be used for source code analysis in pilot 3, to extract the required evidence for the respective metrics.
- What are the expected benefits?
  - The evidence extraction tools are expected to support the identification of security issues in the source code and the identification of non-compliance.
- What are the component-specific requirements?
  - Any identified issues should be supported by enough information to enable a quick reaction by the respective roles.
- Who should have access (roles/permissions) to which results of the component?
  - The evidence should only be accessible to roles which need to see them for their tasks, e.g., an Auditor or a Compliance Manager who are aiming to reach certification for the respective Cloud Service, or a Control Owner working on the respective Metric.

#### 2.3.3.2.7 AI-SEC

- How will the component be used in the pilot?
  - AI-SEC will be used for evidence collection from AI models, specifically regarding robustness against attacks, explainability and fairness.
- What are the expected benefits?
  - Pilot 3 additionally anticipates that the use of the newly developed AI-SEC will support the pilot in gaining a deeper understanding of the current research and novel techniques for the assessment and upcoming audits of AI Models.
- Who should have access (roles/permissions) to which results of the component?
  - The evidence should only be accessible to roles which need to see them for their tasks, e.g., an Auditor or a Compliance Manager who are aiming to reach certification for the respective Cloud Service, or a Control Owner working on the respective Metric.

#### 2.3.3.2.8 EMERALD UI

- How will the component be used in the pilot?
  - The Fabasoft pilot 3 plans to use the EMERALD UI for the whole audit process of the pilot for the agreed upon security schemes. This includes automatic and continuous controls as well as manual controls which have to be audited following the traditional path.
- What are the expected benefits?
  - The pilot expects that the EMERALD UI will allow a seamless interaction with all EMERALD components and their functionalities, and that the EMERALD UI will support the users of the pilot in their audit related processes.
- What are the component-specific requirements?
  - This should help reduce the required resources for reaching certification, support audit related communication and decrease the risk of audit related errors.
- Who should have access (roles/permissions) to which results of the component?

  - Every pilot related role as well as the auditors should be able to use the EMERALD UI. The permissions which were specified for each EMERALD component should be considered in the UI.

#### 2.3.3.2.9 Additional Pilot-specific tool: Fabasoft app.telemetry

- How will the component be used in the pilot?
  - The Fabasoft pilot 3 plans to implement additional evidence collecting tools to integrate pilot-specific applications and tooling into the EMERALD Framework, however this is highly optional.
- What are the expected benefits?
  - As such, the Fabasoft app.telemetry evidence collector integrates the monitoring capabilities of Fabasoft app.telemetry. This integration allows Fabasoft app.telemetry users to use application specific events and data which is collected through Fabasoft's tooling to fulfil requirements needed for certifications.
- Who should have access (roles/permissions) to which results of the component?
  - For this purpose, the Fabasoft app.telemetry evidence collector needs access to the Evidence Store component to import information in a standardized manner. The Evidence Collector will be hosted on Fabasoft's premises. As app.telemetry is not an interactive tool, the evidence which will be provided is the only part that shall be accessible to users – especially metric owners - of the EMERALD framework.

#### 2.3.3.2.10 Additional Pilot-specific tool: Fabasoft Cloud document evidence collector

- How will the component be used in the pilot?
  - The Fabasoft Cloud document evidence collector is an additional pilot specific tool which is used to access documents and meta data that is saved on Fabasoft Cloud.
- What are the expected benefits?
  - This optional evidence collector allows manual controls, signatures and any other relevant meta data which is saved on the Fabasoft PROCECO Cloud to be used as evidence in the EMERALD framework. This is relevant for organizational requirements that focus on policy documents and manual tasks.
- Who should have access (roles/permissions) to which results of the component?
  - For this purpose, the Fabasoft Cloud document evidence collector needs access to the Evidence Store component to import data in a standardized manner. The Evidence Collector will be hosted on Fabasoft's premises. As the Fabasoft Cloud document evidence collector is not an interactive tool, the evidence which will be provided is the only part that shall be accessible to users – especially metrics owners - of the EMERALD framework.

## 2.4 Pilot 4: EMERALD and Hybrid Cloud-Edge environments

This section introduces pilot 4, which is a Category II pilot that aims the certification of hybrid cloud-edge environments for the financial sector.

### 2.4.1 Introduction and Motivation

This pilot 4 aims the certification of hybrid cloud-edge environments for the financial sector. The main driver of this category definition is CaixaBank (CXB), which currently holds a large number of on-premise services and is trying to expand this into the field of public clouds, i.e., using SaaS or IaaS providers. However, due to regulation, there is a need for continuous certification in the sector. The application of EMERALD would ensure the real-time assessment of several cloud services, validating that they are compliant with the controls defined in a specific security framework. Summarized, EMERALD addresses the main challenges of CXB as a customer of cloud and edge service providers. ONS, as a European specialist in managing hybrid cloud-edge environments, will lead this pilot.

**Open Challenges:**

- Security of cloud customer data, in the context of PSD2: Highly regulated industries need to be extra careful in selecting, integrating or on-boarding new cloud and edge services and in assessing them.
- Lack of standardization for interoperability of cybersecurity certification in multi-provider cloud-edge environments: European SaaS providers (e.g., FABA) are interested in providing specialized services, but face high entry barriers.

**Application of EMERALD tool stack**

This Category II pilot will target compliance to the level ‘high’ for continuous certification with the EUCS and will also make use of the EMERALD UI. The specific for Category II is that the EMERALD approach can provide a platform to exchange real-time information of certification states for services within the datacentre-cloud-edge continuum used in the financial sector. More specifically, it offers a secure-by-design application that monitors compliance of services with the same technology on-prem, on the cloud, or at the edge (public or private). This ensures the secure integration of third-party services, guaranteeing their validation of fit-for-purposes.

**Pilot Roles:**

- End-user – CaixaBank
- SaaS – Fabasoft
- IaaS / PaaS – IONOS, CloudFerro
- Cloud-Edge stack – OpenNebula

**Expected general Pilot benefits**

- Proposing a technical implementation that provides answers to the above-mentioned challenges.
- Elaborate on real-time hybrid cloud security, compliance assessment and certification across several cloud and edge infrastructure and service providers.
- Validation of the concepts of WP1 (CaaS framework) and WP4 (user interaction).
- Combined effort for statements on the EMERALD capabilities for hybrid cloud-edge environments.

#### 2.4.1.1 Current Practice and Problem Statement (before EMERALD)

This subsection describes the current situation and the problem, which should be addressed in EMERALD for each of the roles defined in the pilot:

- End-user – CXB
- SaaS – Fabasoft
- IaaS / PaaS – IONOS, CloudFerro
- Cloud-Edge stack – OpenNebula

##### 2.4.1.1.1 End-users – CXB

CaixaBank is one of the leading financial institutions in Spain. Managing a wide array of third-party cloud services that need to be strongly secured and audited for safe-keeping and resilience, necessitating stringent controls and continuous oversight to mitigate risks and comply with regulatory standards.

CXB's current audit process for cloud systems begins with the Service Owner initiating the acquisition of third-party cloud services, detailing the service and data processing locations. This process includes characterization by PGC, gathering risk information from UNED, completing a security questionnaire, identifying applicable controls and generating the evidence matrix, performing risk analysis and control evaluation, and ongoing monitoring and re-evaluation to ensure continued compliance and address changes as needed.

The EMERALD project aims to automate evidence management, enhancing the usability of audit tools, ensuring complete traceability of certificates and audits, and integrating seamlessly with existing internal tools. Additionally, EMERALD will support various certification schemes, allowing CXB to utilize its internal security framework. These initiatives will streamline the audit process, improve efficiency, and ensure compliance with regulatory requirements, addressing the scale, manual processes, and continuous monitoring limitations currently faced by CXB.

##### 2.4.1.1.2 SaaS – Fabasoft

Fabasoft PROCECO is a unique business ecosystem providing selected, powerful and seamlessly integrated solutions for document-intensive business processes. While continuous certification currently imposes several challenges, evidence collection and evidence processing can be fully automated by utilizing existing tools. These can be reused as basis for the Fabasoft pilot 4 participation, with the goal of eventually creating a fully automated audit process and SaaS EMERALD integration.

The product used for this part will be Fabasoft DORA[7]. With Fabasoft DORA, it is possible to create necessary audit reports, such as the information register in accordance with ITS, at the touch of a button and submit them securely to the supervisory authorities. After a positive initial assessment, a standardized review process ensures full compliance with all regulatory requirements. Electronic workflow signatures document every incident in a verifiable manner. The integration of external partners also enables documents and certificates to be submitted without media discontinuity.

Fabasoft believes that this solution is the perfect fit to not only demonstrate the EMERALD capabilities in this pilot, but also showcase the functionalities of an integrated audit support for the financial sector according to the European Digital Operational Resilience Act (DORA).

[7] https://www.fabasoft.com/en/on-proceco/contracts-contract-management/digital-operational-resilience-act

#### 2.4.1.1.3 IaaS / PaaS – IONOS, CloudFerro

IONOS and CloudFerro are participating in pilot 4 of the EMERALD project to advance and integrate state-of-the-art cloud certification technologies tailored for sectors with stringent security demands, such as finance and healthcare. This initiative aims to solidify IaaS and PaaS CSP's position as a leader in secure cloud solutions, enhancing its offerings and demonstrating a commitment to innovation and security in a competitive market. The goal is to cater to the specific requirements of highly regulated industries, which will help attract new customers and retain existing ones.

The predominant challenges include the labour-intensive nature of compliance checks and the cumbersome integration of various systems. These methods not only strain resources but also lead to inefficiencies and a heightened risk of errors, potentially exposing CSPs to legal risks. Furthermore, the current systems do not support real-time compliance monitoring or provide comprehensive visibility across cloud services, which is crucial for swiftly adapting to new regulations. The absence of a unified platform for compliance management complicates transparent reporting and audit trails, which are vital for establishing trust with clients and regulatory authorities.

By addressing these challenges through pilot 4, IONOS and CloudFerro aim to enhance operational efficiency, compliance accuracy, and overall customer trust, aligning with the latest regulatory standards and technological advancements.

#### 2.4.1.1.4 Cloud-Edge stack – OpenNebula

OpenNebula[8] is a powerful European open-source platform to build and manage Enterprise Clouds, which provides unified management of IT infrastructure and applications, avoiding vendor lock-in and reducing complexity, resource consumption and operational costs. It combines virtualization and container technologies with multi-tenancy, automatic provision, and elasticity to offer on-demand applications and services. OpenNebula supports the deployment of hybrid and edge environments with infrastructure resources from different providers (e.g., AWS and Equinix Metal). Additional infrastructure providers can be integrated as long as Terraform[9] Providers exist for them or are developed by the interested stakeholders. For this, a minimum set of functionalities will be defined, in order to guarantee correct interoperability with the rest of the EMERALD stack.

OpenNebula is widely used in enterprise datacentres, and also used by other companies to develop sector-specific, vertical products. All the modifications done in the context of the EMERALD project, therefore, would have an easy way into commercial products. Moreover, OpenNebula, as an open-source project, has a vast community of users that will also benefit from the outcomes of EMERALD. Through EMERALD, OpenNebula is going to Incorporate new features into the OpenNebula platform to provide users and customers with innovative features for cybersecurity certification of multi-provider / hybrid cloud-edge environments.

### *2.4.1.2 Expected Benefits (after EMERALD)*

The benefits expected from EMERALD are the following:

- **Efficiency and availability to certify hybrid cloud-edge environments** within the financial sector: As CXB advances into the integration of SaaS and IaaS with their current on-premise

[8] https://opennebula.io/

[9] https://developer.hashicorp.com/terraform/docs

services, we look forward to ensuring an advance and automated continuous compliance with the rigorous security frameworks required by financial regulations.

- **Real-time Compliance Monitoring:** We expect EMERALD to be capable for real-time compliance monitoring for the hybrid environments to meet high-level EUCS standards.
- **Secure Integration of Services:** With EMERALD, the integration of third-party cloud services can be more secure and agile than nowadays.
- **Overcome Standardization Barriers:** With EMERALD we expect to overcome the lack of standardization in cybersecurity certification across multi-provider environments, facilitating easier entry for specialized service providers.
- **User-friendly UI:** We expect that EMERALD's UI/UX helps auditors and users that monitor the compliance levels and metrics. Allowing a fluid understanding and tracking of the requirements and evidence as well as configurations and other relevant features.

## 2.4.2 Pilot Definition

This section covers the specifications (diagrams and summary) for the pilot definition.

### 2.4.2.1 *General Pilot Diagram*

Figure 11 represents the overall pilot 4 architecture, reflecting the involved EMERALD components, infrastructure, third-party cloud providers and the information flow. It will be analysed in Section 2.4.3 Integration Approach.

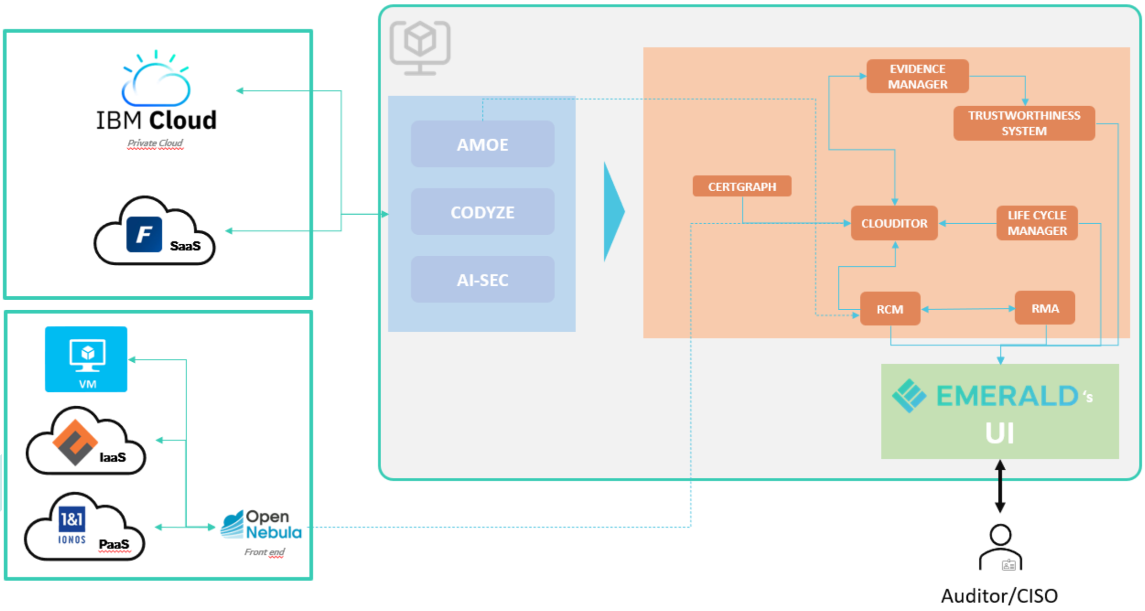


*Figure 11. Overview of the pilot 4 infrastructure*

### 2.4.2.2 *Pilot Hybrid Cloud Deployment Workflow*

For the pilot 4, OpenNebula will be used as a Cloud orchestrator, and the edge capabilities will be provided by the OneProvision module. Figure 12 shows some UML diagrams depicted in the documentation that are just a subset of OpenNebula capabilities relevant for the pilot 4 deployment. The module mainly permits the provision and management of remote edge nodes and clusters.

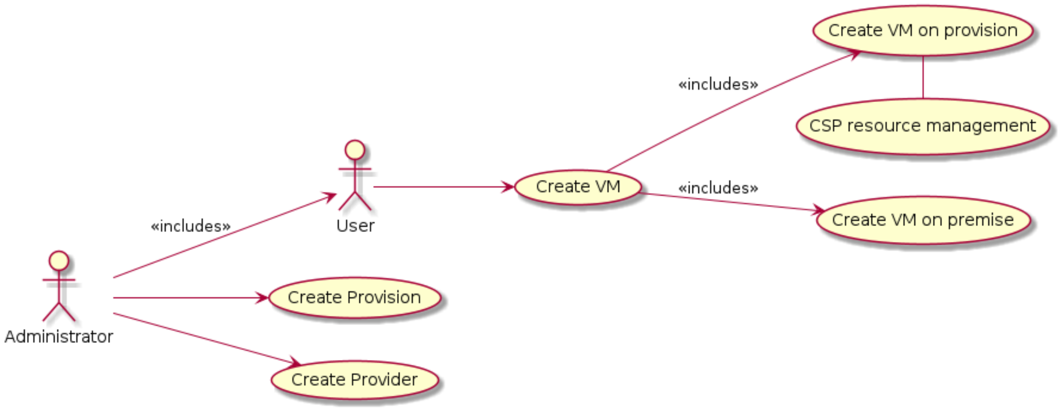


*Figure 12. Pilot 4 use case diagram*

The component diagram in Figure 13 is an overview of the OpenNebula modules involved in the pilot 4 and the IaaS/PaaS CSPs participants interaction.

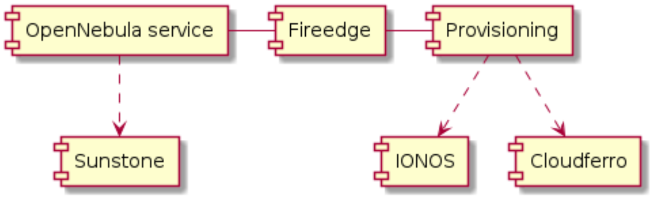


*Figure 13. Pilot 4 Component Diagram*

The sequence diagram in Figure 14 shows the necessary steps to create a new CSP provision.

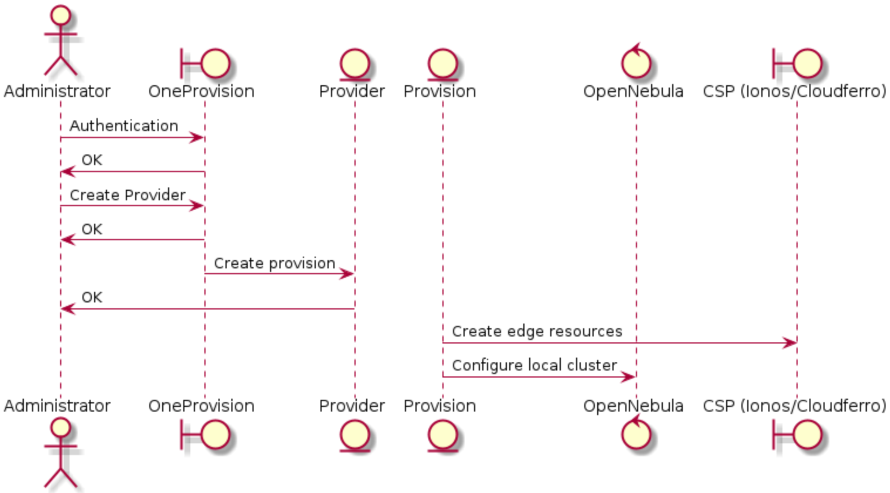


*Figure 14. Sequence diagram between components of the pilot 4*

The main OneProvision's role is the configuration of the external provider(s) that will be used in the pilot. At the moment of writing this report AWS and Equinix are the only supported providers. In this pilot IONOS and CloudFerro will be integrated as CSPs through new drivers over their current bare metal and networking services.

Once the provider has been created, a provision for an edge cluster will be instantiated. The parameters needed for an edge cluster provision will fix the amount of bare metal instances that will be created in the provider and the number of public IPs that will be used to access the remote edge clusters.

The provision of the Edge cluster is made using Terraform[10] and Ansible[11] tools to create the edge cluster and configure it. Because of that, it will be added to the current OpenNebula managed pilot infrastructure.

After that, the following resources will be created locally to use in the edge cluster:

- System and Image datastores
- Virtual network template
- Pool of public cloud IPs

### 2.4.2.3 Hybrid Cloud Architecture Technical requirements

For the pilot 4, OpenNebula Community Edition frontend[12] will be deployed on an on-premise CaixaBank virtual server. There are some networking and security requirements around the multicloud planned environment. Figure 15 represents the main components involved in the deployment and the interaction with EMERALD components.

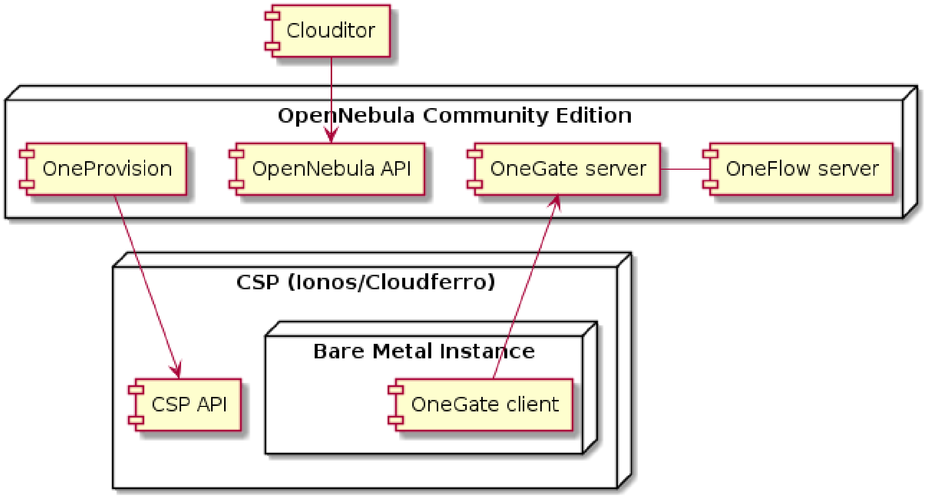


*Figure 15. Block diagram*

OpenNebula network requirements: a valid, authenticated endpoint to the Cloud Service Provider. This will enable the remote cluster deployment features that OpenNebula provides.

Also, EMERALD Clouditor will need access to OpenNebula API in order to validate security policies. A valid AAA (Authentication, Authorization, and Accounting) policy will be defined in OpenNebula in order to provide the associated service providing the infrastructure required data.

[10] https://developer.hashicorp.com/terraform/docs

[11] https://docs.ansible.com/

[12] https://docs.opennebula.io/6.8/intro_release_notes/release_notes_community/what_is.html

### 2.4.2.4 Security controls and measures

The approach to security controls and measures for pilot 4 is currently under development and will be presented in the following deliverables of WP5. The creation of the strategy has to consider the requirements and expectations of each pilot 4 partner.

### 2.4.2.5 Communication and workflow diagram

Figure 16 shows the communication diagram between the assets that OpenNebula provides. The CSP API to integrate the provision engine with IONOS and CloudFerro will be implemented during the project.

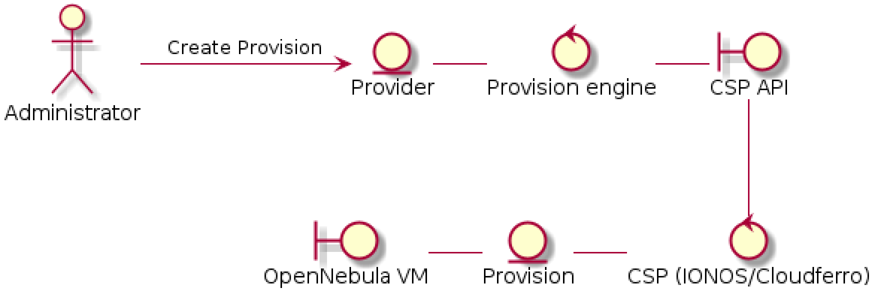


*Figure 16. Communication between entities (1)*

OpenNebula will, as well, implement the necessary API modification to provide Clouditor requirements for the validation of the required security policies, as shown in Figure 17.

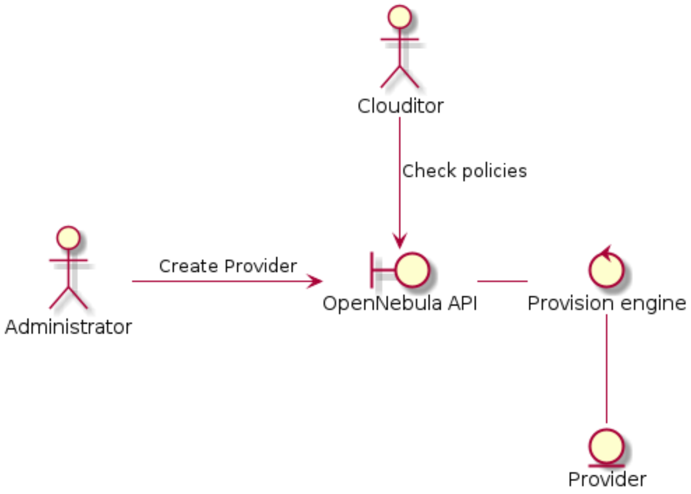


*Figure 17. Communication between entities (2)*

### 2.4.2.6 Business-driven Requirements

Table 5 summarizes the business-driven requirements that describe the requirements of the pilot 4 towards the functionality of the EMERALD framework. The full information can be found in *APPENDIX A: Business-driven requirements*.

*Table 5. Business-driven requirements for pilot 4*

| ID | Name | Description |
|---|---|---|
| BDRP4.01 | Broad Usability & BYOCS (Bring You Own Certification Scheme) | As CaixaBank,<br>we want EMERALD to be able to analyse and check regulatory requirements from different security schemes,<br>so that we can use our own security framework. |
| BDRP4.02 | Enhancing Efficiency and Functionality | As CaixaBank,<br>we want that EMERALD pursues efficiency and functionality,<br>so that the platform performs well and fluidly for the end-users. |
| BDRP4.03 | Ensuring Traceability for Certificates and Audits | As CaixaBank,<br>we want that EMERALD ensures traceability for us as clients and users regarding our certificates and audits,<br>so that we can fully understand and track every requirement and metric to its origin. |
| BDRP4.04 | User-Friendly Interface for All Employees | As CaixaBank,<br>we want that EMERALD has an intuitive UI which is readable for everyone,<br>so that all employees can use it and understand it without high-level skills on legal, compliance or cybersecurity. |
| BDRP4.05 | Integration with Internal Tools | As CaixaBank,<br>we want EMERALD to be able to integrate with CXB internal evidence collector tools,<br>so that we can reuse the components and infrastructure at place. |
| BDRP4.06 | Seamless Migration and Integration | As CaixaBank,<br>we want EMERALD's exploitation and migration to be as smooth as possible integrating all the current service audit/assessment functionalities and requirements,<br>so that we can have an easy transition, increasing services audit/assessment efficiency, decreasing process time and automating initial reports. |
| BDRP4.07 | Documentation | As CaixaBank,<br>we want EMERALD to have a full documentation about the components and the functionalities,<br>so that we can fully understand the tool and components and ease the onboarding for new auditors and tool administrators. |

#### 2.4.2.7 Pilot KPIs

The following KPIs describe the requirements of pilot 4 towards the functionality of the EMERALD framework.

| **KPI** | **4.1 – Automated Compliance Monitoring** |
|---|---|
| **Description** | Measure the ability of EMERALD to monitor compliance in real-time across hybrid cloud-edge environments. |
| **Goal** | Percentage of compliance events detected automatically >90% |
| **Priority** | 1 - must |
| **Benefit** | The automatization and the identification of these compliance guidelines and metrics is crucial for us. I will help in a great measure to accelerate compliance tasks and have a better and continuous control of these environments. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Demonstration workshop |
| **Unit** | Percentage |
| **Baseline value** | No baseline |

| **KPI** | **4.2 - Secure Integration and Compliance** |
|---|---|
| **Description** | Assess the extent to which cloud and edge services are securely integrated and compliant with regulatory standards. |
| **Goal** | Number of compliance breaches identified >90% |
| **Priority** | 1 - must |
| **Benefit** | The automatization and the identification of this evidence is crucial for us. I will help in a great measure to accelerate compliance tasks and have a better and continuous control of these environments. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Demonstration workshop |
| **Unit** | Percentage |
| **Baseline value** | No baseline |

| **KPI** | **4.3 - Standardization of Certification** |
|---|---|
| **Description** | Evaluate the degree to which EMERALD facilitates standardization in cybersecurity certification across multi-provider environments. |
| **Goal** | Number of standardized certifications => 2 certification schemes |
| **Priority** | 2 - should |
| **Benefit** | The ability to be able to run EMERALD with various certifications schemes is important for us in order to be able to exploit it afterwards. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Demonstration workshop |
| **Unit** | Count |
| **Baseline value** | No baseline |

| **KPI** | **4.4 - Validation of Key Concepts** |
|---|---|
| **Description** | Validate the effectiveness of key concepts and frameworks developed for enhancing cloud service integration and user interaction. |
| **Goal** | Success rate of concept validation. Have a user acceptance of 80% of the end users. |
| **Priority** | 2 - should |
| **Benefit** | Having a user validation enhances confidence, fosters adoption and trust. Leading to a smoother integration from the end-users. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Questionnaires |
| **Unit** | Percentage |
| **Baseline value** | Create a baseline with questionnaires |

| **KPI** | **4.5 - User Acceptance** |
|---|---|
| **Description** | Measure the acceptance level of end-users towards EMERALD's functionalities and usability within the financial sector. |
| **Goal** | User satisfaction rating. Increase the compliance capabilities by 20% |
| **Priority** | 2 - should |
| **Benefit** | A successful user acceptance drives productivity, efficiency and satisfaction, which results in a smoother integration and acceptance from the end-users. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Questionnaires |
| **Unit** | Percentage |
| **Baseline value** | Create a baseline with questionnaires |

| **KPI** | **4.6 - Functionality Completion** |
|---|---|
| **Description** | Assess the completion level of functionalities outlined for EMERALD's operation within hybrid cloud-edge environments. |
| **Goal** | Percentage of functionalities completed. 95% |
| **Priority** | 1 - must |
| **Benefit** | In order to ensure an effective operation, streamlining processes and a reduction in change rejection from the end-users. The solutions should mirror the functionalities that were presented to the end-users as much as possible. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Demonstration workshop |
| **Unit** | Percentage |
| **Baseline value** | No baseline |

| **KPI** | **4.7 - Compliance with EUCS Standards** |
|---|---|
| **Description** | Ensure that EMERALD meets high-level EUCS (European Cybersecurity Standard) standard for compliance monitoring. |
| **Goal** | Compliance rate with EUCS standard up to 95% of the high-level compliance regulations |
| **Priority** | 1 - must |
| **Benefit** | Being compliant demonstrates credibility and enhances trust among the users, helps the adoption process and mitigates risks and compliant regulations. |
| **Obstacle** | TBD |
| **Measurement** | |
| **Measured by** | Demonstration workshop |
| **Unit** | Percentage |
| **Baseline value** | No baseline |

### 2.4.3 Integration Approach

Figure 18 shows the planned integration for EMERALD's components into CXB's systems. The EMERALD pilot will be hosted in CXB's Sandbox which presents a safe environment to develop the different tools and interactions between them without extracting any data from the bank premises, which present notorious policies, procedures and bureaucratic processes regarding data protection.

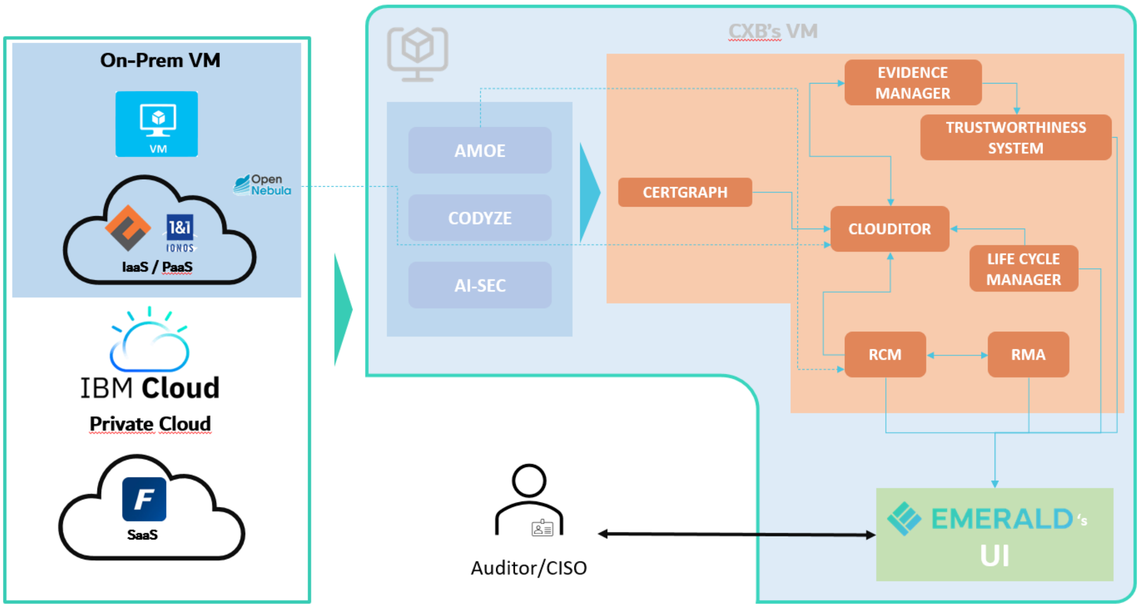


*Figure 18. Pilot 4 Architecture defining all the involved components, infrastructure, third-party cloud services and information flow*

#### 2.4.3.1 Identification of Certification Targets

This section describes the certification targets of pilot 4.

| **Certification Target** | **Cloud Service Provider** |
|---|---|
| **Type** | Third cloud service providers |

| | |
|---|---|
| **Description** | The certification target will be the cloud service provider and the certification will be the own certification schema from CXB generated through other international and EU schemas. |
| **Availability to component owner(s)** | As shown in Figure 18, the specific targets for the pilot will be a VM in CXB's premises, CF and IONOS as IaaS and PaaS respectively. Also, an external private cloud would be IBM's where EMERALD tools will be hosted and finally, Fabasoft as a public cloud service provider in the application layer (SaaS). |
| **Evidence Collection Tool** | **AMOE, AI-SEC and Clouditor-Discovery** |
| **Hosting** | EMERALD |
| **Evidence stored at** | Clouditor – Evidence Store |
| **Evidence processed at** | Evidence Manager |
| **Processed results integrated in** | EMERALD UI |

### 2.4.3.2 *Integration and Application of Components*

This section describes the integration and application of the EMERALD components in pilot 4.

#### 2.4.3.2.1 Clouditor/Orchestrator

- (How) will the component be used in the pilot?
  - Clouditor will be used for continuous monitoring and assessment of cloud resources to ensure compliance with security standards and certification schemes. The main objective of this component is to act as the EMERALD's orchestrator, triggering the needed components to evaluate a requirement based on evidence.
- What are the expected benefits?
  - Continuous and automated monitoring of cloud resources.
  - Enhanced compliance management with reduced manual intervention.
  - Real-time assurance of security controls and configurations.
- What are the component-specific requirements?
  - ORCH.03 - Role Based Access Control
  - ORCH.01 - Final certificate decision
- Where will it be hosted (EMERALD/pilot-specific)?
  - Clouditor will be hosted on the EMERALD platform within the CXB's VM environment.
- Who should have access (roles/permissions) to which results of the component?
  - Auditor/CISO: Full access to compliance reports and monitoring results.
  - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.2 Clouditor-Evidence Store

- (How) will the component be used in the pilot?
  - Clouditor-Evidence Store will be used for storing and managing evidence related to cloud resources and their compliance with security standards and certification schemes. The main objective of this component is to collect, store, and provide access to the evidence required for evaluating compliance requirements within the EMERALD framework.
- What are the expected benefits?
  - Centralized storage of all compliance evidence.
  - Improved organization and retrieval of evidence for audits.

    - Streamlined evidence management, reducing the time and effort required for manual evidence collection.
    - Enhanced traceability and accountability of compliance evidence.
- What are the component-specific requirements?
    - N/A
- Where will it be hosted (EMERALD/pilot-specific)?
    - Clouditor will be hosted on the EMERALD platform within the CXB's VM environment.
- Who should have access (roles/permissions) to which results of the component?
    - Auditor/CISO: Full access to compliance reports and monitoring results.
    - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.3 Trustworthiness System (TWS)

- (How) will the component be used in the pilot?
    - The TWS will be used for secure long-term storage of evidence and assessment results using a Blockchain network. Therefore, ensuring that the evidence hasn't been tampered in any way.
- What are the expected benefits?
    - Enhanced security and integrity of stored evidence and assessment results.
    - Increased transparency and trustworthiness through Blockchain immutability.
    - User-friendly access to evidence via a graphical Blockchain viewer.
- What are the component-specific requirements?
    - TWS.01 - Provide integrity proof of evidence
    - TWS.02 - Provide integrity proof of assessment results
    - TWS.03 - Provide access through REST API or graphical interface
    - TWS.04 - Use a general-purpose public-private Blockchain network
- Where will it be hosted (EMERALD/pilot-specific)?
    - The TWS will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
    - Auditor/CISO: Full access to all stored evidence and assessment results.
    - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.4 Mapping Assistant for Requirements with Intelligence (MARI)

- (How) will the component be used in the pilot?
    - RMA will be used to automatically map requirements from certification schemes to specific metrics using AI techniques.
- What are the expected benefits?
    - Automated, specific and adequate requirement-to-metric mapping.
    - Reduced time and effort in manual mapping processes.
    - Enhanced accuracy and consistency in compliance assessments.
- What are the component-specific requirements?
    - MARI.01 - AI-based
    - MARI.02 - Automatic association
    - MARI.03 - Performance evaluation
    - MARI.04 - Usage and visualization
    - MARI.05 - Strategies
- Where will it be hosted (EMERALD/pilot-specific)?
    - The component will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
    - Auditor/CISO: Full access to all stored evidence and assessment results.

- IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.5 Repository of Controls and Metrics (RCM)

- (How) will the component be used in the pilot?
  - RCM will be used for the storage and management of controls, requirements, metrics, and their relationships.
- What are the expected benefits?
  - Centralized repository for all compliance-related controls and metrics.
  - Streamlined management and retrieval of compliance information.
  - Support for self-assessment and external audits.
- What are the component-specific requirements?
  - RCM.01 - Multi-schema support
  - RCM.02 - Accessible by the rest of components
  - RCM.03 - Include metrics for all schemas supported
  - RCM04 - Mapping of schemes
  - RCM.05 - Import/export of security schemes in OSCAL
  - RCM.06 - Import/export of security schemes in CSV format
  - RCM.07 - GUI to be provided
- Where will it be hosted (EMERALD/pilot-specific)?
  - The component will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
  - Auditor/CISO: Full access to all stored evidence and assessment results.
  - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.6 AMOE

- (How) will the component be used in the pilot?
  - AMOE will be used to extract and assess evidence from organizational policy documents to cover security requirements.
- What are the expected benefits?
  - Automated extraction of evidence from policy documents.
  - Improved coverage of organizational security requirements.
  - Hints and suggestions for compliance based on extracted evidence.
- What are the component-specific requirements?
  - AMOE.01 - Upload PDF document
  - AMOE.02 - Provision of extracted evidence to Evidence Store (Orchestrator/Clouditor)
  - AMOE.03 - Refine evidence extraction approach
  - AMOE.04 - Compare results from multiple documents
  - AMOE.05 - Select metrics per document
  - AMOE.06 - Classify document, select respective metrics (optional)
  - AMOE.07 - Metric states
- Where will it be hosted (EMERALD/pilot-specific)?
  - The component will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
  - Auditor/CISO: Full access to all stored evidence and assessment results.
  - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.7 Codyze and eknows

- (How) will the component be used in the pilot?

  - Codyze and eknows will not be used to perform static code analysis to verify software compliance with security standards and certification schemes as it will be out of the pilot's scope.

#### 2.4.3.2.8 AI-SEC

- (How) will the component be used in the pilot?
  - AI-SEC will be used to analyse ML and AI models for robustness, explainability, and fairness.
- What are the expected benefits?
  - Holistic evidence collection for AI model evaluation.
  - Improved trust in AI models through comprehensive analysis.
  - Enhanced robustness and fairness of AI models.
- What are the component-specific requirements?
  - AI-SEC.01 - Selection of AI Criteria
  - AI-SEC.02 - Selection of AI model
  - AI-SEC.03 - Design the AI-SEC and test it with selected AI Model(s)
  - AI-SEC.04 - Analyse and define the evidence to be extracted
  - AI-SEC.05 - Decide and refine the approach for evidence extraction
- Where will it be hosted (EMERALD/pilot-specific)?
  - The component will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
  - Auditor/CISO: Full access to all stored evidence and assessment results.
  - IT Team: Access for operational insights and compliance maintenance.

#### 2.4.3.2.9 EMERALD UI

- (How) will the component be used in the pilot?
  - The EMERALD UI will be used to provide a reliable, explainable, and trustworthy interface for interacting with the EMERALD components.
- What are the expected benefits?
  - Improved user experience and usability.
  - Centralized access to all EMERALD tools and results.
  - Enhanced transparency and explainability for end-users.
- What are the component-specific requirements?
  - RCM.01 - Multi-schema support
  - RCM.02 - Accessible by the rest of components
  - AMOE.01 - Upload PDF document
  - AMOE.04 - Compare results from multiple documents
  - AMOE.05 - Select metrics per document
  - AMOE.06 - Classify document, select respective metrics (optional)
  - AMOE.07 - Metric states
  - TWS.01 - Provide integrity proof of evidence
  - TWS.02 - Provide integrity proof of assessment results
  - TWS.03 - Provide access through REST API or graphical interface
  - RCM.06 - Import/export of security schemes in CSV format
- Where will it be hosted (EMERALD/pilot-specific)?
  - The component will be hosted on the EMERALD platform, deployed in CXB's VM.
- Who should have access (roles/permissions) to which results of the component?
  - Auditor/CISO: Full access to all stored evidence and assessment results.
  - IT Team: Access for operational insights and compliance maintenance.

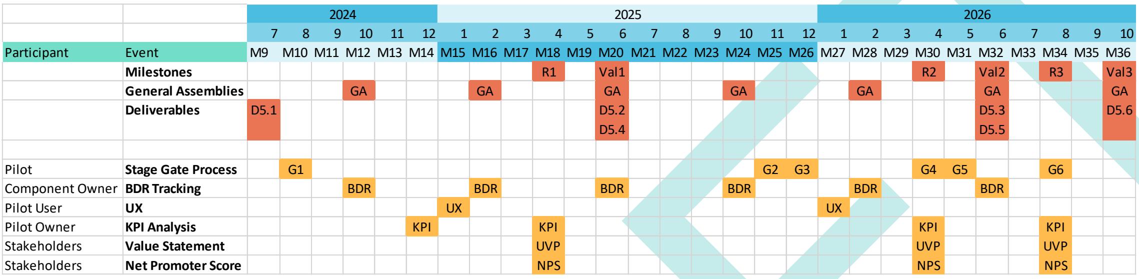
#### 2.4.3.2.10 Additional Pilot-specific tools

- (How) will the component be used in the Pilot?
    - Assessing the possibility to integrate existing evidence collector tools.
- What are the expected benefits?
    - Validate the interconnectivity of the EMERALD framework into CXB's existing environment.
- What are the component-specific requirements?
    - TBD
- Where will it be hosted (EMERALD/pilot-specific)?
    - Pilot-specific infrastructure
- Who should have access (roles/permissions) to which results of the component?
    - TBD

# 3 Validation Plan

The validation plan is expected to cover several aspects of the EMERALD framework and of the individual pilots. Consequently, the plan is rather extensive. It will be executed by the pilots and supported by experts of the individual validation methodologies, as detailed in the specific sections below, and by the component owners of the EMERALD components.

To reduce the burden of validation activities in the pilots, a time plan was created, as shown in Figure 19. This plan can be adapted, considering that validation activities depend on the implementation of the EMERALD framework and different factors related to the pilot partners.



| | | 2024 | | | | | | 2025 | | | | | | | | | | | | 2026 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Participant | Event | M9 | M10 | M11 | M12 | M13 | M14 | M15 | M16 | M17 | M18 | M19 | M20 | M21 | M22 | M23 | M24 | M25 | M26 | M27 | M28 | M29 | M30 | M31 | M32 | M33 | M34 | M35 | M36 |
| | **Milestones** | | | | | | | | | | R1 | | Val1 | | | | | | | | | | R2 | | Val2 | | R3 | | Val3 |
| | **General Assemblies** | | | | GA | | | | GA | | | | GA | | | | GA | | | | GA | | | | GA | | | | GA |
| | **Deliverables** | D5.1 | | | | | | | | | | | D5.2<br>D5.4 | | | | | | | | | | | | D5.3<br>D5.5 | | | | D5.6 |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Pilot | **Stage Gate Process** | | G1 | | | | | | | | | | | | | | | G2 | G3 | | | | G4 | G5 | | | G6 | | |
| Component Owner | **BDR Tracking** | | | | BDR | | | | BDR | | | | BDR | | | | BDR | | | | BDR | | | | BDR | | | | |
| Pilot User | **UX** | | | | | | | UX | | | | | | | | | | | | UX | | | | | | | | | |
| Pilot Owner | **KPI Analysis** | | | | | | KPI | | | | KPI | | | | | | | | | | | | KPI | | | | KPI | | |
| Stakeholders | **Value Statement** | | | | | | | | | | UVP | | | | | | | | | | | | UVP | | | | UVP | | |
| Stakeholders | **Net Promoter Score** | | | | | | | | | | NPS | | | | | | | | | | | | NPS | | | | NPS | | |

Figure 19. Validation time plan

The EMERALD framework has three releases (interim, intermediate, final) and respective deadlines for the validation plan, as documented by the milestones defined in the DoA [1]. These milestones will guide and structure the validation plan:

- MS3 (M18) First release of EMERALD integrated audit suite. First version of the EMERALD business models and plans, communication and dissemination report.
- MS4 (M20) Evaluation of the first release completed.
- MS6 (M30) Second release of EMERALD integrated audit suite
- MS7 (M32) Evaluation of the second release completed.
- MS8 (M34) Final release of EMERALD integrated audit suite.
- MS9 (M36) Evaluation of the final release completed.

To validate the EMERALD framework, the fulfilment of the business-driven requirements (BDR) of each pilot, as well as the EMERALD UI/UX have to be considered. Additionally, the pilot KPIs have to be tracked. To support and finalize the validation, the impact of the EMERALD framework on the different pilots will be monitored and analysed towards the end of the project. This includes forecasting the market impact of the solution through the Impact KPIs, assessing validity of the value statements, and measuring customer satisfaction. Through the Stage-Gate-Process, a “mini audit” will be conducted for each pilot to ensure that EMERALD facilitates the audit scenarios (KPI 8.1[13]).

The results of the validation activities need to be reported back to the technical partners to allow an iterative improvement of the framework. This can be achieved by presenting the results during the General Assemblies (GAs) and through structured documentation in the WP5 deliverables.

[13] From DoA [1]: KPI 8.1 Facilitate at least two different audit scenarios, one for public clouds, one for private cloud installations

In the following sections, the individual validation methodologies are described, including the goal of the validation approach, the expected timeline, the involved parties and the utilization and communication of the results.

## 3.1 Stage-Gate-Process

The progress of the pilots (Task 5.2 and Task 5.3) is driven by a Stage-Gate-Process[14]. The stage in a Stage-Gate process refers to a distinct phase within the project lifecycle in which specific tasks are performed and completed. The Stage-Gate process is divided into several stages, each ending with a "gate." At these gates, the progress of the project is reviewed, and relevant decisions are made to ensure its successful completion.

For EMERALD, the Stage-Gate-Process is defined below and shown in Figure 20. NIXU will be a gatekeeper for each of the gates and will provide the necessary support for the pilots to pass the gates. The use of the Stage-Gate-Process will demonstrate the validity of the developed tools and methodologies and provide valuable feedback to the component owners.

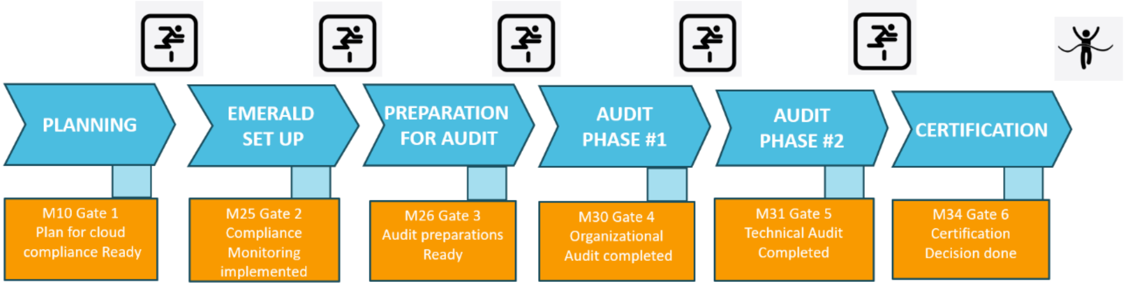

PLANNING
EMERALD SET UP
PREPARATION FOR AUDIT
AUDIT PHASE #1
AUDIT PHASE #2
CERTIFICATION
M10 Gate 1 Plan for cloud compliance Ready
M25 Gate 2 Compliance Monitoring implemented
M26 Gate 3 Audit preparations Ready
M30 Gate 4 Organizational Audit completed
M31 Gate 5 Technical Audit Completed
M34 Gate 6 Certification Decision done

*Figure 20. Stage-Gate-Process*

### 3.1.1 Stage 1: Planning

Stage one of the Stage-Gate-Process ensures that the auditor and the CSP agree on a scope for the audit. The CSP selects a framework, controls, and representatives of the respective roles for the audit process. Additionally, the CSP and the auditor agree on a schedule for the audit.

- **Compliance Manager tasks for the Planning Stage**
  - The pilot nominates a Compliance Manager, who will be responsible for all further compliance tasks in the respective pilot for the Stage-Gate-Process.
  - The pilot defines a compliance framework that is to be pursued during the Stage-Gate-Process.
  - The pilot selects controls from the framework which should be considered for certification (scoping).
  - The pilot decides if continuous audit/certification is required or if the pilot prefers the audit to be a one-time-event.
  - The pilot prepares and presents a schedule for the audit.
  - The pilot performs a RFQ simulation. This means that the pilot will prepare a short request and the auditor will respond with a proposal.
  - The overall plan is approved by the pilots' CISO.
- **Auditor tasks for the Planning Stage**
  - The auditor prepares a work effort estimation according to the defined scope.

[14] https://www.stage-gate.com/blog/the-stage-gate-model-an-overview/

- **Gate**
    - The plan for cloud compliance is ready (M10).

### 3.1.2 Stage 2: EMERALD Setup

Stage two of the Stage-Gate-Process ensures that EMERALD is set up and ready for the audit of each pilot. The required metrics should be implemented at this point, and all necessary EMERALD evidence collection tools are operational.

- **Compliance Manager tasks for the EMERALD Setup Stage**
    - The cloud service is set up and running in a test environment.
    - The organizational and technical metrics are designed and implemented according to the planned scope.
    - The EMERALD tools are operational and collecting evidence according to the scope.
- **Gate**
    - The compliance monitoring is implemented (M25).

### 3.1.3 Stage 3: Preparation for Audit

Stage three of the Stage-Gate-Process ensures that both the CSP and the auditor are ready for the audit. To do so, the CSP has to review and communicate the scope of the audit, complete the self-assessment and share the documentation with the auditor. In the meantime, the auditor nominates a technical auditor and assesses the EMERALD tools and collected evidence.

- **Compliance Manager tasks for the Preparation for Audit Stage**
    - The scope of the audit is communicated to the auditor.
    - The self-assessment has been completed.
    - The organisational and process documentation is shared with the auditor.
- **Auditor tasks for Preparation for Audit Stage**
    - The lead auditor is nominated.
    - The technical auditor is nominated.
    - The validation of the EMERALD framework is performed. Before conducting the audit, an auditor assesses the EMERALD tools and evidence to be used for their trustworthiness and applicability.
- **Gate**
    - The audit preparations are ready (M26).

### 3.1.4 Stage 4: Audit

Stage four of the Stage-Gate-Process includes the organizational and technical audit, which requires the CSP to provide access to the monitoring tools for the auditors. The auditors review the evidence and refer to the CSP's compliance manager for questions.

- **Compliance Manager tasks for the Organizational Audit Stage**
    - An access to the EMERALD compliance monitoring tools is given to the lead auditor.
    - The Compliance Manager is available for questions and has the necessary evidence available for the audit workshop.
- **Auditor tasks for the Organizational Audit Stage**
    - The documentation is reviewed.
    - Organizational controls are assessed according to the scope.
    - An audit workshop is completed with the Compliance Manager.
- **Compliance Manager tasks for the Technical Audit Stage**

  - Access to the EMERALD compliance monitoring is given to the technical auditor.
  - The Compliance Manager is available for questions and has the required evidence prepared for the audit workshop.

- **Auditor tasks for the Technical Audit Stage**
  - The implementation of the technical controls is assessed according to the scope.
  - The technical controls are evaluated for compliance.
- **Gates**
  - The organizational audit is completed. (M30)
  - The technical audit is completed. (M31)

### 3.1.5 Stage 5: Certification

Stage five of the Stage-Gate-Process concludes the audit by resulting in a certification. The auditors identify all non-compliances, communicate the findings and deliver an audit report to the Compliance Manager.

- **Auditor tasks for the Certification Stage**
  - The audit report is delivered to the Compliance Manager
  - Non-compliant controls are identified.
  - All findings are communicated.
- **Gate**
  - The certification decision is done. (M34)

## 3.2 Impact analysis

The impact of the EMERALD framework will be assessed using two dimensions: the Unique Value Proposition (see Section 3.2.1), and the Net Promoter Score (see Section 3.2.2). Both dimensions will be measured using empirical questionnaires targeted for the pilots in M18, M30 and M34 (see Figure 19).

For the EMERALD project, scoring high in both dimensions will enhance the likelihood of achieving market impact in terms of customer engagements. In addition, the EMERALD Impact KPIs [1] (see *APPENDIX B: KPIs and Impact KPIs*) will first be measured with current tools to create baseline values (M14) and then they re-measured using the EMERALD framework after each increment (M18, M30, M34). These KPI values can then be compared between the measurements. The expectation is that there will be an increase in efficiency that will contribute, for example, to cost savings.

The main stakeholders for the EMERALD project results are the auditors from the certification approval body, as well as Compliance Managers and CISOs of the pilot CSPs. The plan is to use the project members in respective roles to execute the validation plan.

### 3.2.1 Empirical questionnaire analysing the validity of the value statement

The value statement in a Lean Canvas, also known as the Unique Value Proposition (UVP), is a clear and concise statement that outlines the unique benefit or value that a product provides to its target customers. This statement differentiates the product from its competitors and explains why customers should choose it over other alternatives.

To create value statements for EMERALD, each component owner will be asked to create value statements for their own component. Some examples will be prepared to support the component owners. Subsequently, EMERALD stakeholders (see section 3.2) will be asked to evaluate if they agree with the statements on a 5-point LIKERT scale (Strongly disagree, Disagree, Neutral, Agree, Strongly agree).

The value statements of the individual components will be evaluated at each increment of the components (M18, M30, M34), to ensure timely feedback (see Figure 19). This allows the component owners to react immediately and work towards improving their score.

### 3.2.2 Empirical questionnaires analysing customer satisfaction

The Net Promoter Score (NPS)[15] is a widely used market research metric that gages customer loyalty and satisfaction. NPS serves as a concise measure of how likely customers are to recommend a company's products or services to others. NPS is based on the fundamental perspective that customers can be divided into three categories:

- **Promoters:** customers who are satisfied and will refer others (9-10)
- **Passives:** customers who are satisfied but are open to competitive offerings (7-8)
- **Detractors:** customers who are dissatisfied and generate negative word-of-mouth (0-6)

To assign a customer to a category, they are asked how likely they are to recommend the brand or product to a friend or colleague, on a scale from one to ten. Customers who have answered zero to six are considered Detractors, customers who have answered seven or eight are considered Passives and customers who have answered nine or ten are considered Promoters. Each component owner is a subject for Net Promoter score (NPS) measurement where stakeholders will answer how likely they will recommend the solution to a friend or colleague.

The NPS is calculated by subtracting the percentage of Detractors from the percentage of Promoters (% Promoters - % Detractors = NPS). The score is not expressed as a percentage but as an absolute number lying between -100 and +100. Customer satisfaction will be evaluated at each increment of the EMERALD framework (M18, M30, M34), as shown in Figure 19.

### 3.2.3 Impact KPI measurement

The expected impact will be measured using the impact KPIs (see *APPENDIX B: KPIs and Impact KPIs)*, which were defined in the DoA [1]. Each pilot will perform a measurement of the impact KPI: a) with the currently used traditional/current methods/tools for reaching certification, and b) then again with EMERALD methods and tools at different points in time.

To guarantee a common approach towards the measurement of the impact KPIs, instructions for the measurement tasks, and tables for the tracking of values will be prepared. An example for this can be found in *APPENDIX C: Impact KPI measurement example*. It has to be considered that the example is still work in progress and prone to change. Each pilot owner will be asked to follow this measurement plan. It is foreseen that the instructions are aligned with the scenarios developed in WP4, to guarantee that they can be followed in the EMERALD UI for the measurement of the KPIs. Furthermore, the component owners will be required to support the pilot owners as needed if their component is directly or indirectly involved in the tasks.

Impact KPIs will be measured at each increment of the EMERALD development (M18, M30, M34), as well as in M14, to achieve a baseline value (see Figure 19). The KPIs in M14 are measured without using the EMERALD framework. As a result, the measurement of these KPIs should be adapted to the needs of each pilot, while still following the instructions for subsequent measurements as closely as possible.

[15] https://www.netpromoter.com/know/

The pilots will then analyse the collected impact KPI measurements. If the impact KPI target could not be achieved for one or more pilot owners, the pilot owners will provide feedback to the component owners.

## 3.3 Pilot KPI analysis

Pilot KPIs were elicited by the individual pilots in Task 5.1. They are presented in the respective section "Pilot KPIs" for each pilot in Section 2. To track and analyse these KPIs, each pilot should measure the initial KPIs with current audit processes and methods at the beginning of the project.  After every release of the EMERALD Framework (M18, M30, M34) the KPIs should be measured again, using the current version of the EMERALD tools. The initial measurement can then be compared to the final measurement in M34, while the measurements of M18 and M30 can be used to recognize and counteract any deviations (see Figure 21).

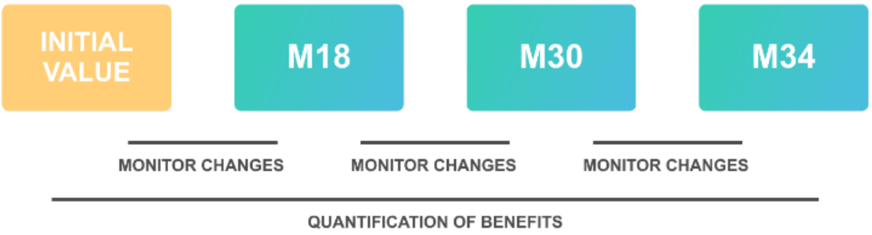


*Figure 21. Pilot KPI analysis*

As each pilot has different KPIs and even similar KPIs will be measured differently by the individual pilots, the purpose of these KPIs is to show how the individual pilots can benefit from the use of EMERALD, not to compare the different pilots. The KPIs will be measured by each pilot owner. The improvement between measurements can then be reported in absolute or relative numbers, depending on the pilots' preferences and security guidelines.

To ensure that the component owners have all relevant information to consider the KPIs during component implementation, pilot owners will evaluate whether KPIs are represented in the technical requirements or whether pilot owners still need to create technical requirements in WP1.

## 3.4 Fulfilment tracking of business-driven requirements

The business-driven requirements were elicited by the individual pilots in Task 5.1. They are presented in the respective section "Business-driven requirements" for each pilot in Section 2. The business-driven requirements have to be implemented in the respective components. To ensure the technical feasibility of the implementation and to assign the correct component owners, the business-driven requirements were reviewed in collaboration with WP1 and then translated into or mapped to one or more technical requirements for each relevant component (see Figure 22). Each technical requirement has a field "validation criteria" which has to be reviewed by the pilot owners. This helps to ensure that the technical requirement fulfils the expectations of the pilots regarding the business-driven requirement.

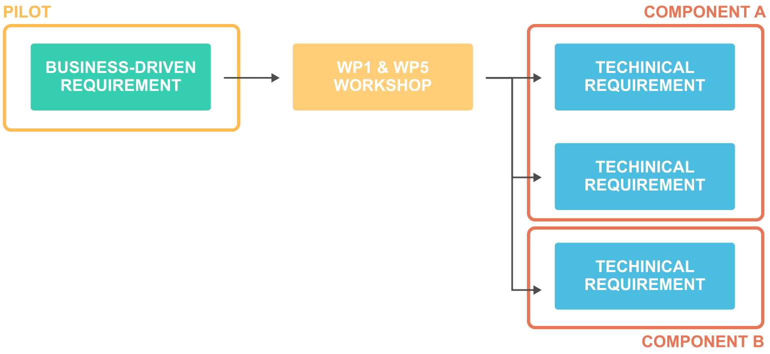


*Figure 22. Translation of requirements for implementation*

To track the implementation of the respective technical requirements, business-driven requirements will be reviewed at or around the time of a General Assembly (see Figure 19), where each owner of a technical requirement related to a business-driven requirement will be asked to give a short, written statement on the implementation, feasibility and any issues arising in relation to the technical requirement. If necessary, the technical requirement may be changed to guarantee a satisfactory implementation for the pilots (see Figure 23). This will be documented and reported in each of the following WP5 deliverables.

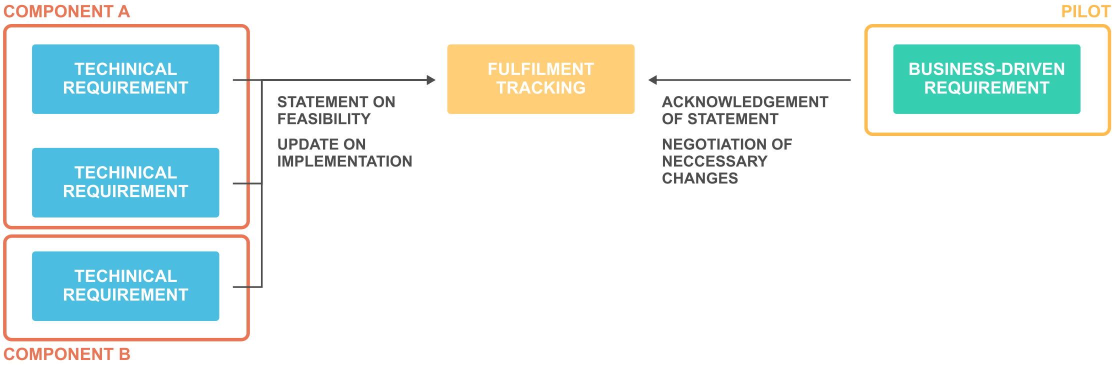


*Figure 23. Fulfilment tracking of business-driven requirements*

## 3.5 UX Validation

The goal of the UX validation is to ensure an easy-to-use interface for the EMERALD users, which supports transparency regarding the EMERALD algorithms, and to reinforce the user centric approach. As a result, the main focus of the UX validation is to provide feedback on the concept and implementation of the user interface (usability & transparency) and on the EMERALD components (transparency & functionality).

This feedback has to be provided in time to allow for relevant changes in the user interface concept and the components. To enable an iterative development of the user interface and its concept, the UX validation has two iterations. The first iteration is planned for the beginning of the second year of the project, and the second for the beginning of the third year. After each iteration, how to improve the usability and transparency of the user interface should be evaluated, based on the results, in a collaborative effort between WP4 and WP5. While the second iteration will be conducted using the already implemented EMERALD user interface, the first iteration will be based on the mock-ups created in WP4.

For the UX validation a mixed methods approach will be applied: Thinking Aloud [2], System Usability Scale (SUS) [3], and a concluding interview. These methods are described below. For each iteration, the pilot partners are asked to provide participants for the UX validation. These participants should work as one of the EMERALD roles, so that input from relevant sources can be collected.

An iteration of the UX validation is expected to take between one and two hours per participant, depending on the extent of the to-be-developed user interface. It is envisaged that the UX validation will be conducted through team calls. The meeting will start with a short introduction briefing participants about EMERALD and the upcoming session. For this purpose, a participation information sheet, a consent form and a data protection sheet will be prepared. This will be followed by the think-aloud user test, followed by the SUS questionnaire. The UX validation will conclude with a short interview, in which the participant will have the opportunity to share their final thoughts on the UI and the EMERALD framework.

### 3.5.1 Thinking Aloud

Thinking aloud is a usability testing method where participants are asked to use the designed system, while continuously voicing their thoughts on the experience. To ensure that all relevant user interface features are tested and that the results are comparable, the tasks to be performed during the test are prepared.

For the UX validation of EMERALD, participants will receive tasks based on the workflows prepared by WP4. At this stage, the UI concept is under development, so it is not possible to predict how the UI can be best used. The WP4 workflows will describe how a user should use EMERALD and are therefore the optimal basis for these tasks. Participants will be asked to perform the tasks and to continuously voice their thoughts. Meanwhile, EMERALD UX experts will record the session and take additional notes. The experts will remind the participants to continue their monologue, if necessary, but will not otherwise interfere during the session.

After the sessions, the recordings and notes will be reviewed, and the insights documented. The summarized results will then be discussed with WP4 to provide feedback for the development of the user interface. The evaluation will focus not only on the usability of the user interface, but also on the transparency of the overall EMERALD framework, as perceived through the user interface.

### 3.5.2 System Usability Scale

The System Usability Scale (SUS) [3] is a questionnaire consisting of 10 items that are rated on a 5 point-Likert scale (from strongly disagree (1) to strongly agree (5)) to measure the subjective experience of the usability of a system. It is used after participants have used the system but before any discussion regarding the system has happened. The results of the SUS can then be used to compare the usability of a system to similar systems and to compare different iterations of the same UI. The SUS was translated to several languages. To guarantee consistent results, the original version by John Brooke [3] in English will be used:

1. I think that I would like to use this system frequently
2. I found the system unnecessarily complex
3. I thought the system was easy to use
4. I think that I would need the support of a technical person to be able to use this system
5. I found the various functions in this system were well integrated
6. I thought there was too much inconsistency in this system
7. I would imagine that most people would learn to use this system very quickly
8. I found the system very cumbersome to use

9. I felt very confident using the system
10. I needed to learn a lot of things before I could get going with this system

For the UX validation of EMERALD, participants will be asked to fill in this questionnaire immediately after concluding the Thinking Aloud method. The results will be documented and, after the second iteration, used to ensure that the usability of the EMERALD UI has increased.

### 3.5.3 Interview

A semi-structured interview is the last part of the UX validation. It should debrief the participants and offer the chance to discuss any open points which arose during the UX validation.

# 4 Conclusions

This deliverable introduces the four EMERALD pilots from Category I and Category II. The summarized goals of the pilots are as follows:

**Pilot 1** by IONOS aims at enhancing Public Infrastructure as a Service (IaaS) through the EMERALD framework. As a prominent European cloud provider, IONOS is set to advance continuous certification processes crucial for meeting dynamic cybersecurity standards by integrating the EMERALD tools into its public IaaS. This integration shifts compliance management from traditional methods to an automated, real-time monitoring system, enhancing operational efficiency and security while boosting customer trust. The deliverable details the roles, interactions, and workflows necessary for a systematic deployment of this pilot, setting IONOS up to demonstrate an automated certification model in a large-scale public cloud environment. This initiative positions IONOS to not only strengthen its market leadership but also drive the evolution of cloud security standards across Europe, maintaining its edge in technological and regulatory compliance.

**Pilot 2** by CloudFerro aims at testing tools in IaaS/PaaS environment on public cloud. CF will provide resources on its public cloud and prepare IaaS and PaaS test environments, which will be used for evidence collection by the EMERALD tools (hosted at EMERALD not at the pilot itself). Evidence will be also gathered from documentation (policies, etc.). The goal for the pilot is the automation of the certification process (especially documentation verification) resulting in cost reduction of an audit.

**Pilot 3** by Fabasoft attempts to integrate all EMERALD tools. The goal of this pilot is to achieve an assisted certification with the EUCS high level requirements and to evaluate the applicability of the pilot findings to a BSI C5 audit. For this purpose, the EMERALD framework will be used, and a selected set of metrics will be addressed. Additional metrics and controls, which are not part of the continuous audit, should be managed manually through the EMERALD user interface, to allow a full coverage of the catalogues. For this, the Fabasoft pilot sets up a test environment which can be certified by the EMERALD's CaaS approach.

**Pilot 4** provides a detailed technical analysis of the current challenges and the collaborative efforts being undertaken in the EMERALD project to address them in hybrid cloud environments. For CaixaBank (CXB), automating evidence management and audit processes will enhance security and regulatory compliance in managing third-party cloud services. Fabasoft's integration of EMERALD into its PROCECO ecosystem aims to fully automate audit processes, showcasing the capabilities of the platform in meeting the European Digital Operational Resilience Act (DORA) requirements. IONOS and CloudFerro are focusing on advancing cloud certification technologies to meet the high security demands of finance and healthcare sectors, addressing the inefficiencies in current compliance practices. OpenNebula, as an open-source platform, is enhancing its features to support cybersecurity certification in multi-provider and hybrid cloud-edge environments, benefiting both its enterprise users and the broader community. Overall, these efforts demonstrate a concerted push towards innovation, efficiency, and compliance in complex cloud and edge computing environments.

This deliverable also provides a guideline for the validation of EMERALD and its pilots. These plans outline how the validation should be approached by the pilots and the technical work packages to provide iterative feedback to the implementation of the EMERALD framework. Through the presented time plan it is ensured that there is enough time for the pilots and the technical work package to create, review and implement this feedback for each iteration of the EMERALD framework during the project.

The results of the validation as well as further information on the pilots will be presented in the deliverables D5.2 “Category I pilot validation-v1” (M20), D5.3 “Category I pilot validation-v2” (M32) , D5.4 “Category II pilot validation-v1” (M20), D5.5 “Category II pilot validation-v2” (M32) and D5.6 “Evaluation report and impact analysis” (M36).

# 5 References

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

[2] W. Wirth, S. Wolf, U. Mögerle and S. Böcking, “Measuring the subjective experience of presence with think-aloud method: Theory, instruments, implications,” *Proceedings of the Seventh Annual International Workshop on Presence,* pp. 351-358, October 2004.

[3] J. Brook, “SUS: A quick and dirty usability scale,” *Usability Eval. Ind.,* November 1995.

# APPENDIX A: Business-driven requirements

This appendix contains the description of the business-driven requirements that have been elicited by the EMERALD pilots. Each requirement is presented in a table which was created to collect all relevant information. Next to the requirement ID, short title and description, the status and priority of the requirement are documented. Additionally, the involved components, the source of the requirement (Pilots/Component/DoA/KPI) and their type (Technical/Pilots/GUI) is collected. In addition, each requirement is linked to at least one KR and KPI and contains validation acceptance criteria, to further specify which outcome is expected.

| **Requirement ID** | BDRP1.01 |
|---|---|
| **Short title** | Automate and Streamline Certification Processes |
| **Description** | As IONOS pilot 1,<br>we want the certification process to be automated,<br>so that the time spent on manual entries can be reduced and we focus more on strategic compliance planning. |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | Clouditor |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_EXTRACT |
| **Related KPI** | KPI 1.1 |
| **Validation acceptance criteria** | Certification process time is reduced without any increase in compliance issues |

| **Requirement ID** | BDRP1.02 |
|---|---|
| **Short title** | Secure and Reliable Long-term Evidence Storage |
| **Description** | As IONOS pilot 1,<br>we need a system that securely stores all compliance evidence long-term,<br>so that we can retrieve it quickly and reliably for any audits or compliance checks without fearing data loss or corruption. |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | TWS |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR2: CERTGRAPH |
| **Related KPI** | KPI 2.1 |
| **Validation acceptance criteria** | No failures in annual data integrity checks following implementation |

| **Requirement ID** | BDRP1.03 |
|---|---|

| | |
|---|---|
| **Short title** | Efficient Requirement and Compliance Mapping |
| **Description** | As IONOS pilot 1,<br>we want to use an AI-assisted mapping tool to quickly align our service offerings with multiple compliance frameworks, ensuring accuracy and saving time on cross-referencing standards manually. |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | MARI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR3_OPTIMA |
| **Related KPI** | KPI 3.2 |
| **Validation acceptance criteria** | Compliance mapping is completed faster than the current average with no loss in accuracy |

| | |
|---|---|
| **Requirement ID** | BDRP1.04 |
| **Short title** | Central Management of Controls and Metrics |
| **Description** | As IONOS pilot 1,<br>we need a central repository where we can easily manage and update security controls and metrics,<br>so that changes are propagated accurately and timely across all compliance documentation and reports. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | RCM |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR2_CERTGRAPH |
| **Related KPI** | KPI 2.1 |
| **Validation acceptance criteria** | Data retrieval times during audits are reduced compared to baseline values |

| | |
|---|---|
| **Requirement ID** | BDRP1.05 |
| **Short title** | Compliance Verification for Organizational Policies |
| **Description** | As IONOS pilot 1,<br>we want a tool that can automatically assess our organizational policies against compliance standards,<br>so that we can easily identify and address gaps in our internal policies without manually reviewing each one. |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | AMOE |

| | |
|---|---|
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_Extract |
| **Related KPI** | KPI 1.1 |
| **Validation acceptance criteria** | Reduction in compliance gaps identified during audits compared to baseline |

| | |
|---|---|
| **Requirement ID** | BDRP1.06 |
| **Short title** | Ensure Software Compliance through Static Code Analysis |
| **Description** | As IONOS pilot 1,<br>we need a static code analysis tool that integrates into our CI/CD pipeline to verify compliance before deployment, ensuring that any compliance issues are caught and resolved early in the development process |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | CODYZE |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_Extract |
| **Related KPI** | KPI 1.1 |
| **Validation acceptance criteria** | Static code analysis detects more compliance issues pre-deployment than current tools. |

| | |
|---|---|
| **Requirement ID** | BDRP1.07 |
| **Short title** | Intuitive User Experience for Compliance Monitoring |
| **Description** | As IONOS pilot 1,<br>we want a user-friendly interface that allows to monitor compliance status across various cloud services easily,<br>so that we can make quick decisions based on real-time data and effectively communicate compliance status to stakeholders. |
| **Status** | Proposal |
| **Priority** | Must |
| **Components** | EMERALD UI/UX |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6_EMERALD UI/UX |
| **Related KPI** | KPI 6.3, KPI 6.4 |
| **Validation acceptance criteria** | User satisfaction with the new UI/UX is rated higher in user surveys |

| | |
|---|---|
| **Requirement ID** | BDRP2.01 |
| **Short title** | OpenStack |
| **Description** | As CloudFerro,<br>I want EMERALD to be able to gather evidence collection about resources from OpenStack (including Magnum for PaaS),<br>so that we can use it. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | See GitLab |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR8 |
| **Related KPI** | KPI 8.1 |
| **Validation acceptance criteria** | EMERALD can be fully used with OpenStack. |

| | |
|---|---|
| **Requirement ID** | BDRP2.02 |
| **Short title** | Reusable Metrics & Requirements |
| **Description** | As CloudFerro,<br>I want that a requirement or metric which was already implemented can be reused,<br>so that the audit time can be decreased. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | EMERALD UI, RCM |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR4 |
| **Related KPI** | KPI 4.1 |
| **Validation acceptance criteria** | After a user has set up a metric or requirement, this metric or requirement can be reused to measure the same thing in a different security certification scheme. |

| | |
|---|---|
| **Requirement ID** | BDRP2.03 |
| **Short title** | Transparency increase |
| **Description** | As CloudFerro,<br>I want that EMERALD increases transparency for our clients and users about our certificates and audits,<br>so that we can ensure to our clients that our services are secured properly. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | TWS, Clouditor-Orchestrator |
| **Source** | Pilots |
| **Type** | Pilots |

| | |
|---|---|
| **Related KR** | KR7 |
| **Related KPI** | KPI 7.1 |
| **Validation acceptance criteria** | It has to be easy to understand for users how and why the audit results were reached.<br>It has to be easy to understand for users, which certificates are issued. |

| | |
|---|---|
| **Requirement ID** | BDRP2.04 |
| **Short title** | Intuitive UI |
| **Description** | As CloudFerro,<br>I want that EMERALD has an intuitive UI which is readable for everyone,<br>so that even non-technical employees like compliance managers can use it without problem. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | EMERALD UI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6 |
| **Related KPI** | KPI 6.2, KPI 6.3 |
| **Validation acceptance criteria** | A non-technical employee, like a compliance manager, can successfully use the UI without technical support. |

| | |
|---|---|
| **Requirement ID** | BDRP2.05 |
| **Short title** | Security Schemes |
| **Description** | As CloudFerro,<br>I want EMERALD tools to certify BSI-C5 (must), ISO 27001 (could), BSI 200-1 (could),<br>so that EMERALD can support us with certificates we already use. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | RCM |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR4, KR7 |
| **Related KPI** | KPI 4.1 |
| **Validation acceptance criteria** | - |

| | |
|---|---|
| **Requirement ID** | BDRP3.01 |
| **Short title** | UI/UX Concept |
| **Description** | As Fabasoft pilot 3,<br>we want a well-crafted UI/UX concept,<br>so that our users perceive EMERALD as an intuitive audit solution. |

| | |
|---|---|
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | EMERALDUI, Clouditor-Orchestrator |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6_EMERALD UI/UX |
| **Related KPI** | KPI 6.3 |
| **Validation acceptance criteria** | A complete UI/UX concept is available which can be used to craft the User Interface of EMERALD.<br>For better understanding, UI/UX concept is clearly explained and can be used without support. |

| | |
|---|---|
| **Requirement ID** | BDRP3.02 |
| **Short title** | AI Guideline |
| **Description** | As Fabasoft pilot 3,<br>we want to be educated on areas of application for AI in certification-as-a-service environments with the help of EMERALD's well-structured AI guidelines,<br>so that we can reproduce this in future use cases. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | AI-SEC |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR5_AIPOC |
| **Related KPI** | KPI 5.1, KPI 5.2 |
| **Validation acceptance criteria** | A well-structured AI guideline is available which can also be used for future use cases. The guideline educates on areas of application for AI in certification-as-a-service environments. |

| | |
|---|---|
| **Requirement ID** | BDRP3.03 |
| **Short title** | Integration of Internal evidence collection tools |
| **Description** | As Fabasoft pilot 3,<br>we want to integrate our internal evidence collection tools (e.g., Fabasoft app.telemetry),<br>so that we can use and reuse the extracted evidence in the CaaS and exploit the opportunity to have our tool as a valid evidence extractor. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | Clouditor-EvidenceStore |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_EXTRACT, KR2_CERTGRAPH |
| **Related KPI** | KPI 1.1, KPI 2.1 |

| | |
|---|---|
| **Validation acceptance criteria** | It is possible to use internal evidence collection tools as valid evidence extractors. The collected evidence through the internal evidence collector can be used and reused in EMERALD. |

| | |
|---|---|
| **Requirement ID** | BDRP3.04 |
| **Short title** | Reusable Metrics |
| **Description** | As Fabasoft pilot 3,<br>we want to use EMERALD's reusable metrics,<br>so that the audit process is simplified. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | RCM, EMERALDUI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR4_MULTICERT |
| **Related KPI** | KPI 4.1 |
| **Validation acceptance criteria** | After a user has set up a metric, this metric can be reused to measure the same thing in a different security certification scheme. This metric is suggested to the user, when the second certification scheme is looked at, so that the user does not have to remember that this metric exists and measures the relevant information already. |

| | |
|---|---|
| **Requirement ID** | BDRP3.05 |
| **Short title** | Security Schemes pilot 3 |
| **Description** | As Fabasoft pilot 3,<br>we want to manage Fabasoft's audit (BSIC5 (must), EUCS (must), AIC4 (must)) through the application of EMERALD,<br>so that resource consumption is minimized. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | Clouditor-Assessment, EMERALDUI, RCM |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR4_MULTICERT, KR7_INTEROP |
| **Related KPI** | KPI 4.1 |
| **Validation acceptance criteria** | The BSI C5 audit is supported by EMERALDs tools and processes. |

| | |
|---|---|
| **Requirement ID** | BDRP3.06 |
| **Short title** | Custom set of requirements |
| **Description** | As Fabasoft pilot 3,<br>we want to manage an audit process based on an individual set of requirements – e.g., originating from a cloud customer as planned in pilot 4, |

| | |
|---|---|
| | so that Fabasoft is able to address specific cloud customer needs as seen in the financial sector. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | EMERALDUI, RCM |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR3_OPTIMA, KR4_MULTICERT, KR6_EMERALD UI/UX, KR7_INTEROP |
| **Related KPI** | KPI 3.2, KPI 3.3, KPI 4.1, KPI 6.2, KPI 7.1, KPI 7.2 |
| **Validation acceptance criteria** | It is possible to create a custom set of requirements in a custom collection.<br>It is possible to publish this collection.<br>It is possible for other CSPs to assign this collection to them and to publish the results of the audit to the issuer of this collection (or to another party). |

| | |
|---|---|
| **Requirement ID** | BDRP3.07 |
| **Short title** | Enhance current audit process |
| **Description** | As Fabasoft pilot 3,<br>we want to understand how we could transfer our current audit process to EMERALD and enhance them by this change,<br>so that we understand the benefits of EMERALD and estimate any efficiency increase. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | EMERALDUI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6_EMERALD UI/UX |
| **Related KPI** | KPI 6.1, KPI 6.2, KPI 6.3 |
| **Validation acceptance criteria** | There is a workflow or similar which describes how the current audit process can be transferred to EMERALD. The UI supports the User through this workflow. |

| | |
|---|---|
| **Requirement ID** | BDRP3.08 |
| **Short title** | Audit Transparency |
| **Description** | As Fabasoft pilot 3,<br>we want to utilize EMERALD functionality,<br>so that the audit transparency is increased. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | Clouditor-Assessment, Clouditor-Orchestrator, TWS |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR7_INTEROP |

| | |
|---|---|
| **Related KPI** | KPI 7.1 |
| **Validation acceptance criteria** | It has to be easy to understand for users how and why the audit results were reached |

| | |
|---|---|
| **Requirement ID** | BDRP3.09 |
| **Short title** | Manual Controls |
| **Description** | As Fabasoft pilot 3,<br>we want EMERALD to have a strategy on how manual controls can be included in an automated audit (e.g., in the UI),<br>so that a complete audit can be supported by EMERALD. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | EMERALDUI, Clouditor-Assessment, Clouditor-EvidenceStore, Clouditor-Orchestrator |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR8_PILOTS, KR2_CERTGRAPH, KR4_MULTICERT |
| **Related KPI** | KPI 8.1 |
| **Validation acceptance criteria** | It is not necessary for CSPs to use multiple Systems for their audit processes. EMERALD supports the automated controls, but also allows the management of controls with have to be done manually (documentation, communication w. auditor, setting of appropriate status...). |

| | |
|---|---|
| **Requirement ID** | BDRP3.10 |
| **Short title** | Safe security scheme updates |
| **Description** | As Fabasoft pilot 3,<br>we want to be aware if there is a relevant update in a security scheme we use and we want to be able to safely transfer to the new version,<br>so that we do not lose our certification or my data when we choose to update the scheme. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | RCM, Clouditor-Orchestrator |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR7_INTEROP |
| **Related KPI** | KPI 7.2 |
| **Validation acceptance criteria** | User gets information when the security scheme needs to be updated. User can choose when to do it and user can do it in a way where they will not temporarily loose the certification |

| | |
|---|---|
| **Requirement ID** | BDRP3.11 |
| **Short title** | Checks for policy documents |

| | |
|---|---|
| **Description** | As Fabasoft pilot 3,<br>we would like to see if the policy document is containing the relevant information according to the requirements,<br>so that we can be sure all organisational requirements are covered, and we do not have to search the document manually. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | AMOE, EMERALDUI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_Extract, KR6_EMERALD UI/UX |
| **Related KPI** | KPI 1.1, KPI 6.3 |
| **Validation acceptance criteria** | The user shall upload a document and is able to see how many requirements x/y are done. Also, the user shall be able to view which parts are ok / not ok.<br>The user shall see if a document is providing relevant evidence when looking at a certain metric. |

| | |
|---|---|
| **Requirement ID** | BDRP3.12 |
| **Short title** | Use of standard for export/import |
| **Description** | As Fabasoft pilot 3,<br>we want to be able to use a known standard for the export and import of information from and to the EMERALD framework,<br>so that this is easily possible where needed. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | RCM, EMERALDUI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR7_INTEROP |
| **Related KPI** | KPI 7.1 |
| **Validation acceptance criteria** | Information can be imported and exported from EMERALD using a known standard. |

| | |
|---|---|
| **Requirement ID** | BDRP4.01 |
| **Short title** | Capacity to be able to identify any type of certification schema within the scope of the project |
| **Description** | As CaixaBank,<br>we want EMERALD to be able to analyse and check regulatory requirements from different security schemes,<br>so that we can use our own security framework. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | AMOE; RCM |
| **Source** | Pilots |

| | |
|---|---|
| **Type** | Pilots |
| **Related KR** | KR4_MULTICERT; KR7_INTEROP |
| **Related KPI** | KPI 4.1, KPI 4.2, KPI 7.1, KPI 7.2 |
| **Validation acceptance criteria** | In order to validate this requirement, EMERALD must be able to identify and analyse any certification schema within the project's scope, allowing CaixaBank to use its own security framework. Testing EMERALD's components to ensure they can accurately interpret and check regulatory requirements from various security schemes, meeting all defined acceptance criteria. |

| | |
|---|---|
| **Requirement ID** | BDRP4.02 |
| **Short title** | Ensure EMERALD platform delivers high efficiency and smooth functionality for optimal end-user performance. |
| **Description** | As CaixaBank,<br>we want that EMERALD pursues efficiency and functionality,<br>so that the platform performs well and fluidly for the end-users. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | AI-SEC; AMOE; Clouditor-Orchestrator; Codyze; eknows; EMERALDUI; Clouditor-EvidenceStore; RCM; RMA; TWS |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6_EMERALD UI/UX; KR7_INTEROP; KR8_PILOTS |
| **Related KPI** | KPI 6.1, KPI 6.2, KPI 6.3, KPI 7.1, KPI 7.2, KPI 8.2 |
| **Validation acceptance criteria** | To validate this requirement the platform must respond to user actions within few seconds for all interactions. The initial load time of the platform should not exceed normal timing on a standard broadband connection. Finally, the platform should maintain performance benchmarks under peak load conditions. |

| | |
|---|---|
| **Requirement ID** | BDRP4.03 |
| **Short title** | Ensure EMERALD provides complete traceability of certificates and audits, enabling full tracking of requirements and metrics to their origin. |
| **Description** | As CaixaBank,<br>we want that EMERALD ensures traceability for us as clients and users regarding our certificates and audits,<br>so that we can fully understand and track every requirement and metric to its origin. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | Clouditor-Orchestrator; Clouditor-Assessment; TWS |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR7_INTEROP; KR8_PILOTS |
| **Related KPI** | KPI 7.1, KPI 7.2, KPI 8.2 |

| | |
|---|---|
| **Validation acceptance criteria** | EMERALD must provide complete traceability of certificates and audits, enabling users to understand the automated decisions and rules used by the AI models. Users should be able to replicate all the steps taken by the EMERALD tool.<br>The validation could include testing Clouditor-Orchestrator, Clouditor-Assessment, and TWS components to ensure that every requirement and metric can be tracked to its origin, and all decision-making processes are transparent and reproducible, with documented results meeting the acceptance criteria. |

| | |
|---|---|
| **Requirement ID** | BDRP4.04 |
| **Short title** | Enable EMERALD with a user-friendly interface, ensuring all employees can navigate and comprehend it without highly-specialized knowledge. |
| **Description** | As CaixaBank,<br>we want that EMERALD has an intuitive UI which is readable for everyone,<br>so that all employees can use it and understand it without high-level skills on legal, compliance or cybersecurity. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | EMERALD-UI |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR6_EMERALD UI/UX |
| **Related KPI** | KPI 6.2, KPI 6.3 |
| **Validation acceptance criteria** | To validate this requirement, we propose that employees can navigate and understand without specialized knowledge in legal, compliance, or cybersecurity. Validation includes usability testing with a diverse group of employees, ensuring the UI is intuitive and accessible, with positive feedback on ease of use and comprehension, meeting all defined acceptance criteria and documenting the results. |

| | |
|---|---|
| **Requirement ID** | BDRP4.05 |
| **Short title** | Ensure that EMERALD's components are able to integrate with CXB's internal evidence collector tools, allowing reuse of existing components and infrastructure such as endpoint agents. |
| **Description** | As CaixaBank,<br>we want EMERALD to be able to integrate with CXB internal evidence collector tools,<br>so that we can reuse the components and infrastructure at place. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | Clouditor-Evidence Store; Clouditor-Orchestrator |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR1_EXTRACT |

| | |
|---|---|
| **Related KPI** | KPI 1.1, KPI 1.2 |
| **Validation acceptance criteria** | EMERALD must integrate with CXB's internal evidence collector tools, reusing existing components and infrastructure such as endpoint agents. Validation includes testing integration with Clouditor-Evidence Store and Clouditor-Orchestrator, ensuring seamless functionality, reusability of components, and compatibility with existing infrastructure, meeting all defined acceptance criteria and documenting results. |

| | |
|---|---|
| **Requirement ID** | BDRP4.06 |
| **Short title** | The EMERALD Framework should be gracile enough to facilitate smooth exploitation and migration for end-users, integrating current audit functionalities to enhance efficiency, reduce process time, and automate initial reports. |
| **Description** | As CaixaBank,<br>we want EMERALD’s exploitation and migration to be as smooth as possible integrating all the current service audit/assessment functionalities and requirements,<br>so that we can have an easy transition increasing services audit/assessment efficiency, decreasing process time and automating initial reports. |
| **Status** | Proposed |
| **Priority** | Must |
| **Components** | N/A |
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | KR8_PILOTS |
| **Related KPI** | KPI 8.2 |
| **Validation acceptance criteria** | The framework must integrate current audit functionalities seamlessly, enhance service audit efficiency, reduce process time, and automate initial report generation. Validation includes user acceptance testing, efficiency measurement, process time analysis, and continuous monitoring, ensuring all criteria are met and documented. |

| | |
|---|---|
| **Requirement ID** | BDRP4.07 |
| **Short title** | Provide full documentation of EMERALD's components and functionalities to enhance understanding and ease onboarding for new auditors and administrators. |
| **Description** | As CaixaBank,<br>we want EMERALD to have a full documentation about the components and the functionalities,<br>so that we can fully understand the tool and components and ease the onboarding for new auditors and tool administrators. |
| **Status** | Proposed |
| **Priority** | Should |
| **Components** | All |

| | |
|---|---|
| **Source** | Pilots |
| **Type** | Pilots |
| **Related KR** | N/A |
| **Related KPI** | N/A |
| **Validation acceptance criteria** | Documentation should cover all components of EMERALD as well as the tool itself in a clear and understandable language. Plausible Measurements:<br>- Review the documentation to ensure it includes detailed descriptions, usage guidelines, and interactions for each component in EMERALD.<br>- Conduct usability tests/pilots with auditors to evaluate their understanding and ease of onboarding using the documentation and user manuals. |

# APPENDIX B: KPIs and Impact KPIs

This is the list of **KPIs** that have been defined in the DoA [1]:

- **KPI 1.1:** Provide support for evidence extraction from different sources (infrastructure, code, processes)
- **KPI 1.2:** Provide novel methods for the security assessment of AI models and their evidence generation
- **KPI 2.1:** Provide a schema for storing and linking heterogeneous evidence information
- **KPI 2.2:** Provide support traceability to information sources and extraction processes
- **KPI 2.3:** Provide scalability for storing/processing continuously collected evidence; demonstrated in the pilots
- **KPI 3.1:** Provide scheme to scheme mapping functionality based on metrics, recommended to the user
- **KPI 3.2:** Provide metric-to-requirement-mapping functionality by improving MEDINA approaches and incorporating KPI 5.1 results
- **KPI 3.3:** Provide insights for the mapping decision and how the recommendation process works
- **KPI4.1:** Provide realizable metrics that demonstrate compliance to at least two security certification schemes
- **KPI 4.2:** Provide metric assessment for 80 % of the metrics in KPI 4.1 based on the certification graph
- **KPI 5.1:** Provide realizable metrics to help evaluate at least 50% of the categories of criteria of the BSI AIC4 that deal with the robustness of ML system, their interpretability, and the mitigation of potentially negative impacts such as model unfairness (c.f. Chapter 6, AIC4).
- **KPI 5.2:** Provide a PoC for semi-automated assessment of 80% of the metrics specified in KPI 5.1.
- **KPI 6.1:** Provide roles and workflows, derived from interviews with relevant users (e.g., project partners and advisory board members), develop mock-ups and interaction concepts for managing the audit process
- **KPI 6.2:** Provide concept for the (UI) of EMERALD and integration of evidence collection components, data bases and orchestrating components
- **KPI 6.3:** Provide a graphical user interface for role-based access to certification information content
- **KPI 7.1:** Conventionalize import and export functionalities to take or share data with external sources
- **KPI 7.2:** Incorporate input from standardisation bodies and synchronize data formats and protocols
- **KPI 8.1:** Facilitate at least two different audit scenarios, one for public clouds, one for private cloud installations
- **KPI 8.2:** Validate user acceptance in terms of complexity reduction
- **KPI 9.1:** Dissemination, communication and exploitation strategy set-up with a viable business model of EMERALD identified by M18 and revised by M36
- **KPI 9.2:** Standardization roadmap identified by M18 and revised by M36, guidance on OSCAL and a set of metrics for the EUCS forwarded to ETSI, ENISA, CIS, NIST and BSI

This is the list of **Impact KPIs** that have been defined in the DoA [1]:

- **KPI EI1.1:** Decrease the effort (measured in hours / person) needed by the Cloud Services to incorporate updates of the certification schemes and re-certificate

- **KPI EI1.2:** Decrease the time needed to identify common controls among certification schemes by 50% compared to the current values
- **KPI EI1.3:** The satisfaction degree of AI teams with the application of the EMERALD approach and tools to the AI scope is of at least 85%. This data will be collected by means of questionnaires or surveys, following the SUST methodology.
- **KPI EI2.1:** Decrease the time needed to (self) certify cloud services in 30% compared to the current values
- **KPI EI2.2:** The satisfaction degree of different types of users with the customized views and layers of the EMERALD solution is at least of 85%
- **KPI EI3.1:** The identified stakeholders (national agencies, cloud service providers, customers and auditors) are covered by the EMERALD approach
- **KPI EI4.1:** The effort needed to map different security schemes is decreased in 30%
- **KPI EI4.2:** Decrease the time needed to find services compliant with a certain assurance level by 50% compared to the current values.
- **KPI EI5.1:** The source code is released in public OSS repositories (e.g., Project's public Gitlab, OW2, others) in accordance with the freemium business model and IPR
- **KPI EI6.1:** Decrease on the time needed for the identification and realization of security metrics related to different security controls by 30%

# APPENDIX C: Impact KPI measurement example

The following approach for measuring KPI EI1.2 is an example of the current work in progress for the measurement and tracking of the impact KPIs.

| **KPI EI1.2** | | |
|---|---|---|
| Decrease the time needed to identify common controls among certification schemes by 50% compared to the current values | | |
| **Month** | **Value** | **Note** |
| M14 | | Time estimated by experienced employees |
| M18 | | Time measured when using EMERALD |
| M30 | | Time measured when using EMERALD |
| M34 | | Time measured when using EMERALD |

## Prerequisites

**Pilot**: A user is ready for the mapping of controls and metrics between security schemes.

**EMERALD**: A cloud service is set up for the pilot in EMERALD which already has one certification scheme with existing controls and metrics. At least two security schemes are available which have similar controls.

**Auditor**: no actions required]

## Validation

The time is measured starting with the moment the user opens the second certification scheme until the user correctly maps an existing metric to a new control. It is recommended to repeat this process several times for more accurate values:

1. Analyse the two (or more) schemes involved. In this case, these could be known schemes or unknown ones.
2. Focus on the first control which is relevant for the analysis we are performing in scheme 1.
3. Look for a similar set of controls in scheme 2.
4. Once a candidate or set of candidates are identified in scheme 2, assess if they can be considered as "common" controls.
5. Repeat this for all the controls in scheme 1 until all the common controls are found.