Deliverable D4.2

Results of the UI-UX requirements analysis and the work processes – v2

Editor(s):	Angela Fessl, Katharina Stefan
Responsible Partner:	Know Center Research GmbH
Status-Version:	Final – v1.0
Date:	30.04.2025
Type:	R
Distribution level (SEN, PU):	PU

Project Number:	101120688
Project Title:	EMERALD

Title of Deliverable:	D4.2 Results of the UI-UX requirements analysis and the work processes – v2
Due Date of Delivery to the EC	30.04.2025

Workpackage responsible for the Deliverable:	WP4 - User interaction and user experience development
Editor(s):	Angela Fessl, Katharina Stefan (KNOW)
Contributor(s):	Simone Franza, Leonie Disch (KNOW) Björn Fanta, Franz Deimling, (FABA) Julius Holderer (IONOS) Ramon Martin de Pozuelo, Marti Fabregat I Pous (CXB) Natalia Sobieska (CF) Mika Leskinen, Antti Kantero (NIXU/DNV)
Reviewer(s):	Olivia Kagerer (FABA) Juncal Alonso, Cristina Martínez (TECNALIA)
SAB Reviewer(s):	Samu Nisula (NIXU/DNV) Marti Fabregat (CXB) Björn Fanta (FABA) Sebastian Kucharski (CF) Ali Nikoukar (IONOS) Constantino Vázquez (ONS)
Approved by:	All Partners
Recommended/mandatory readers:	WP1, WP2, WP3, WP5, WP6

Abstract:	Final version of the report on the elicited UI-UX requirements from the target group. Work processes and workflows that should be covered with the user interface concept, and final personas and scenarios.
Keyword List:	UI/UX Requirements, Works Processes, Personas, Scenarios
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	23.03.2025	First draft version	Angela Fessl, Katharina Stefan (KNOW)
v0.1	01.04.2025	QA review	Olivia Kagerer (FABA)
v0.2	02.04.2025	Feedback integration of QA review	Angela Fessl, Katharina Stefan (KNOW)
v0.3	03.04.2025	Feedback integration and review with TECNALIA	Cristina Martinez (TECNALIA)
v0.4	03.04.2025	Feedback integration of TECNALIA review	Angela Fessl, Katharina Stefan (KNOW)
v0.5	03.04.2025	SAB Review	Samu Nisula (NIXU/DNV) Marti Fabregat (CXB) Björn Fanta (FABA) Sebastian Kucharski (CF) Ali Nikoukar (IONOS) Constantino Vázquez (ONS)
v0.6	14.04.2025	SAB Review Integration	Angela Fessl (KNOW)
v0.7	22.04.025	Final Review	Juncal Alonso, Cristina Martínez (TECNALIA)
v0.8	23.04.2025	Addressing the comments from Final Review	Angela Fessl (KNOW)
v1.0	30.04.2025	Submitted to the European Commission	Juncal Alonso, Cristina Martínez (TECNALIA)

Table of contents

List of Tables

List of figures

Terms and abbreviations

AI	Artificial Intelligence
AMOE	Bring Your Own Certification Scheme
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
C5	Cloud Computing Compliance Criteria Catalogue
CaaS	Compliance-as-a-Service[1]
CM	Compliance Manager
CSP	Cloud Service Provider
CSV	Comma-separated value
DoA	Description of Action
DORA	Digital Operational Resilience Act
EC	European Commission
ECB	European Central Bank
EUCS	European Union Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
ICO	Internal Control Owner
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KR	Key Result
MARI	Mapping Assistant for Regulations with Intelligence
MS Teams	Microsoft Teams
RCM	Repository of Controls and Metrics
SaaS	Software as a Service
SAB	Security Advisory Board
SO	Service Owner
SOC	Security Operations Center frameworks
SP	Service Provider
TRL	Technology Readiness Level
UI	User Interface
UNED	Universidad Nacional de Educación a Distancia (National University of Distance Education)
UX	User Experience

[1] Please note that in previous deliverables and in the DoA, the term Certification-as-a-Service was used to stand for CaaS. Compliance has now been introduced to clarify that EMERALD can be used to assess both normative models and internal organizational models.

Executive Summary

The EMERALD UI/UX (user interface/user experience) offers the user interface (UI) and user experience (UX) to address Compliance as-a-Service[2] (CaaS) and its continuous and lean re-certification aspects with a focus on the user's needs. The goal is to develop a concrete user interaction concept that leads to a fully-fledged UI/UX for EMERALD.

This deliverable D4.2 is the extended version of D4.1 [1], which was released in M9. D4.2 is related to *WP4 - User interaction and user experience development* and presents the final results regarding *T4.1 - Requirements engineering with compliance managers and auditors* and *T4.2 - Modelling work processes*. The document describes the final methodology that we applied in WP4, which includes the requirement analysis conducted, the final results derived regarding the work processes and workflows, the personas and scenarios, and the complete set of UI/UX requirements relevant for implementing the EMERALD UI/UX.

In more detail, in this deliverable we present, first, the results of the interactive interview session to get insights about the pilot partners' needs. Second, we present the final results of the elicited work processes and workflows and how they could be enhanced by using the EMERALD UI. Third, we included the final set of personas and corresponding scenarios. And finally, we present the elicited UI/UX requirements. Our main findings can be summarized as follows:

- We were able to **derive concrete work processes** per **pilot partner** and for **external auditors and compliance managers** from NIXU/DNV. These processes present the preparation and execution of audits from the perspective of compliance managers, security managers, and auditors. These include the stakeholders' working tasks, which information and data they need to do their tasks, and how the EMERALD solution could support them.
- We derived a **universally applicable blueprint for implementing EMERALD** that is valid for all pilots and that can support the audit preparation and audit execution workflows. This blueprint may be valuable for other companies seeking to use the EMERALD solution to enhance their audit preparation processes or to support audit executions.
- We have developed three stakeholder groups including seven personas: the **compliance stakeholders** consisting of **2 different compliance manager personas** and **1 internal control owner persona;** the **technical stakeholder** consisting of **1 technical implementer; and** the **auditor stakeholders** consisting of **3 different auditor personas**. For each of the personas, we have developed "personas-on-the-go" which are a concise visual summary highlighting key characteristics of each persona. Additionally, we have developed **16 detailed scenarios** to understand the work of all stakeholder groups in more detail. The personas and scenarios helped us to understand the roles and tasks of compliance managers, auditors, and technical stakeholders. This is essential for designing a system that effectively supports certification preparation and audit execution and for identifying the key functionalities needed in the EMERALD UI to support all stakeholder groups.
- Finally, we were able to elicit **25 UI/UX requirements** for developing the EMERALD UI/UX, covering the most relevant functionality that the EMERALD UI should provide.

[2] Please note that in previous deliverables and in the DoA, the term Certification-as-a-Service was used to stand for CaaS. Compliance has now been introduced to clarify that EMERALD can be used to assess both normative models and internal organizational models

1 Introduction

In this deliverable we present the final results of task *T4.1 – Requirements engineering with compliance managers and auditors* and *T4.2 – Modelling work processes.*

This document is the successor of D4.1 [1], which presented the initial insights gained about the processes and workflow, the personas and scenarios as well as the elicited requirements for the EMERALD UI. Section 1.3 presents the modifications of this document compared of D4.1 [1].

1.1 About this deliverable

One of the project's objectives as defined in the DoA [2] is:

"***O3: Provide a seamless user experience of continuous auditing for auditors and auditees****: The EMERALD project aims at providing a concept on how to approach the audit process and view the data in a suitable and intuitive way. This includes descriptions of roles for the different users involved (e.g., compliance manager, internal control owner, auditor, …), development of a concept for the integration of components and data related to the certification process and building a unique overview platform for certification stakeholders.*"

To facilitate this, we have used and applied different methods for the EMERALD UI/UX development, consisting of four major elements:

- **Research Methodology**: The overall methodology of WP4 follows a co-design, participatory and contextual design approach. With this approach we aimed at deriving the final UI/UX requirements, the target groups' final work processes, and the final set of personas and scenarios. We conducted different activities consisting of interviews, focus groups, workshops, and iterative meetings with pilot partners, external auditors and component owners.
- **Work processes and workflows**: We conducted eight interviews, four focus groups and seven process workshops to derive the final work processes and iteratively refined and improved them throughout the course of the project. This resulted in ten simple processes and ten elaborated workflow representations. Additionally, we developed a blueprint representation combing the major insights from the individual processes.
- **Personas and Scenarios**: From four persona and scenario workshops, we were able to derive seven individual personas representing three stakeholder groups and 16 respective scenarios.
- **UI/UX Requirements**: Finally, we elicited 25 UI/UX requirements from interviews, focus groups and workshops. These requirements cover the most important views and functionalities that the EMERALD UI/UX must offer to the target users.

The target audience of this deliverable is twofold:

- First, all EMERALD partners: This deliverable addresses the technical partners, because their components and the corresponding outputs will be connected to and presented in the EMERALD UI, as well as the pilot partners, since their employees -including compliance managers, internal control owners and auditors-, are the target groups of EMERALD.
- Second, this document is also targeted to the broader EMERALD target users (e.g., potential end-users, strategic partners, communities, or policymakers) who might be interested in socio-technical design, co-creation and co-design. For them, this document provides some guidance and concrete examples on how to elicit knowledge from different stakeholders with various backgrounds (e.g., interviews, focus groups). It

presents how to carry out a UI/UX development process that corresponds to the needs and wishes of the target users.

The goal of this deliverable is to present the applied methodology, the requirement analysis, as well as the final results, which are summarized below:

- the result of the active interview session serving as starting point for EMERALD providing us first insights about the **pilots' audit preparation processes** in general, their **needs**, some **pain points** and **expectations** towards EMERALD;
- the final **concrete work** of the pilot partners and the auditors and compliance managers from NIXU/DNV[3] about the audit preparation and the audit execution, including working tasks, information and data they need to do their tasks, and how the EMERALD solution could be used to support them;
- a **universally applicable blueprint for implementing EMERALD** in audit preparation and audit execution workflows, which may be valuable for other companies seeking to use the EMERALD solution to enhance their audit preparation processes or to support audit executions;
- the seven **final personas** and "**personas-on-the-go**, as well as **16 scenarios**; they helped us to understand the roles and tasks of compliance managers, auditors, and technical stakeholders and serve as baseline for implementing the EMERALD user administration;
- the final set of the **25 UI/UX requirements** necessary for the design and development of the EMERALD UI.

1.2 Document structure

The document is structured as follows:

After the introduction section, Section 1, Section 2 presents the whole methodology used for fulfilling the objectives of Tasks 4.1 and 4.2.

Section 3 summarizes the findings of the interactive interview session held at the general assembly in Bilbao. Section 4 presents the final processes and workflows elicited from the interviews, focus groups, and process workshops conducted with the pilot partners and external auditors. Section 5 presents all personas, "personas-on-the-go" and scenarios developed. Section 6 summarizes the final set of UI/UX requirements derived from all the activities conducted (e.g., interviews, focus groups, workshops) including their progress status. Additionally, a full description of the new added requirements since M9 is presented. Finally, Section 7 concludes the report.

[3] In 2023, DNV acquired Nixu, a Finnish cybersecurity firm, through a public tender offer.
Following the acquisition, DNV merged Nixu with its existing cybersecurity business and another acquired company, Applied Risk, to form a new entity branded as DNV Cyber, effective mid-2024.
This merger combined Nixu's expertise in IT and managed cybersecurity services, Applied Risk's specialization in industrial control systems, and DNV's knowledge of critical infrastructure industries.
The goal was to create one of Europe's fastest-growing cybersecurity service providers, addressing rising cyber risks within critical industries and offering comprehensive cybersecurity solutions to them.
In the EMERALD Proposal, NIXU is named as part of the EMERALD consortium – referred to here as NIXU/DNV. NIXU/DNV provides deep insights into the world of cybersecurity service providers, they represent the auditor stakeholders in EMERALD and provide crucial insights into how audits are conducted and what needs to be considered in EMERALD in this regard.

APPENDIX A: Interview Documents includes the interview guideline, the participant information sheet, the consent form, and the data protection sheet.

APPENDIX B: Original User Scenario Descriptions contains the initial scenario descriptions derived from the workshops in form of figures. During the course of the project, some scenarios have had to be changed due to technical feasibility or implementation considerations. If there were discrepancies between the textual description and the corresponding figure, the figure was placed directly beneath the scenario description. If no adaptations were made regarding the scenario description and the created figures, the figures are included in the appendix.

APPENDIX C: UI/UX Requirements elicited before M9 presents the UI/UX requirements that have been elicited before M9.

1.3 Updates from D4.1

This deliverable evolves from D4.1 [1]. Our ultimate goal is to make the final and current version of D4.2 self-contained. Therefore, several unchanged sections have been directly taken over from D4.1. Other parts that have been developed during the last nine months are new. To simplify the tracking progress and updates from the previous version, Table 1 briefly summarises the changes and additions to each section of the document.

Table 1. Overview of deliverable updates with respect to D4.1

Section	Changes
Section 1: Introduction	It is based on the text from D4.1 but enhanced with the new achievements and results.
Section 2: Methodology	The methodology section was updated accordingly from D4.1 and presents the overall methods used for the whole tasks conducted in T4.1 an T4.2.
Section 3: Results of the Interactive Interview Session	This was taken over from D4.1 without any changes.
Section 4: Work Processes	The work processes have been completely elaborated for all pilot partners and NIXU/DNV (auditors and compliance manager).
Section 4.1: Work Processes in Workflow Presentation	This section is new and describes the workflow representation in general.
Section 4.2.1: Pilot 1: IONOS	This section is new and describes the simple processes and the workflow representation of the audit preparation process for IONOS.
Section 4.2.2: Pilot 2: CloudFerro	This section is updated: in D4.1 we presented only the simple processes for an audit preparation at CloudFerro. This section is now extended and also covers the corresponding workflow representations.
Section 4.2.3: Pilot 3: Fabasoft	This section is updated: in D4.1 we presented the simple processes for an audit preparation at Fabasoft. This section is now extended and covers the corresponding workflow representations.

Section	Changes
Section 4.2.4 **Pilot 4: CaixaBank**	This section is new and describes the simple processes and the workflow representation of the audit preparation process for CXB.
Section 4.2.5: Auditors (NIXU/DNV)	This section is updated: in D4.1 we presented the simple processes for an audit process of an auditor from NIXU/DNV. This section is now extended and covers the corresponding workflow representations.
Section 4.2.6: Compliance Manager (NIXU/DNV)	This section is updated: in D4.1 we presented the simple processes for an audit preparation process of a compliance manager from NIXU/DNV. This section is now extended and covers the corresponding workflow representations.
Section 4.3: Blueprint for introducing EMERALD in audit preparation	This section is new and describes the derived blueprint for implementing EMERALD in audit preparation and audit execution workflows.
Section 5: Personas	In D4.1, we presented the following four personas: • Emerson - Compliance Manager in Financial Service Institution • Riley – Cloud Service Provider Compliance Manager • Dylan – Internal Control Owner • Charlie – Internal Auditor The following three new personas have been added: • Morgan – Technical Implementer • Jarkko – Lead Auditor • Eero – Technical Auditor
Section 5: **“Personas-on-the-go”**	Additionally, we have presented for each persona a condensed and easy-to-understand “persona-on-the-go”.
Section 5: Scenarios	In D4.1, we presented the following three scenarios: • Scenario 1: Emerson – Bring Your Own Certification Scheme • Scenario 2: Dylan – Internal Control Owner Control Implementation • Scenario 3: Charlie – Preparation of an Audit by an Internal Auditor In D4.2, we have added the following 13 scenarios: • Scenario A: Riley – Managing a New Audit Scope • Scenario B: Riley – Manage all Controls of an Audit Scope • Scenario C: Riley – Uncover all “blind spots” • Scenario D: Riley – Updating a certification scheme • Scenario E: Riley – Accompanying an Audit • Scenario A: Morgan – Checking Metrics and Evidence • Scenario B: Morgan – Removal of Metric Removal of Metric • Scenario A: Jarkko – Scoping • Scenario B: Jarkko – Preparing for Audit

Section	Changes
	• Scenario C: Jarkko – Organizational Audit • Scenario D: Jarkko – Certification • Scenario A: Eero – Technical Audit • Scenario B: Eero – Reporting
Section 6: UI/UX Requirements (version 2)	We present for all requirements the progress regarding the development of the clickable prototype of the EMERALD UI.
Section 6.1: Newly Added UI/UX Requirements since M9	This section covers new requirements for the EMERALD UI/UX that we have added since M9: we present the detailed description as well as the current progress of the development regarding the clickable prototype of the EMERALD UI.

2 Methodology

The overall methodology of WP4 follows a co-design, participatory and contextual design approach (see [3], [4], [5], [6]) using different methods such as interviews, focus groups, and workshops. Such a co-design approach aims at bridging the gap between technology designers, developers, and target users. Terms like co-design, participatory and contextual design highlight similar concepts, emphasizing the active involvement of all stakeholders to meet both the individual and organizational needs [7]. Participatory design is also seen as an emancipatory act, allowing users to have a say in the tools they use [6]. Co-creation involves shared creativity [5], while co-design applies this creativity throughout the entire design process. Active user participation throughout development is encouraged, creating a hybrid space that combines user and developer attributes. This shift from "user as subject" to "user as partner" has changed stakeholder roles [5], with users potentially becoming meta-designers and researchers acting as facilitators. Co-design is characterized by iterative learning processes involving all stakeholders.

Goal: We have decided to use co-design as an overall methodology for the WP4 activities. We see this approach as a viable means to bridge the gap between EMERALD technology partners and EMERALD pilot partners to develop a sophisticated EMERALD UI/UX. Thereby, the aim of the co-design is:

- to get a good understanding of the underlying processes and workflows regarding the preparation and implementation of audits and the certification of cloud services,
- to elicit a set of requirements for developing the EMERALD UI/UX,
- to develop personas, scenarios, and user journeys (presented in D4.3 [8] and D4.4 (M24)), and
- to develop a full-featured clickable prototype of the EMERALD UI.

We conducted the elicitation process iteratively to continuously involve the target groups throughout the different activities and processes, gather their feedback and insights, and allow their input to be integrated on the fly. The final goal is to design a sophisticated EMERALD UI that integrates the needs of all involved parties (pilot partners – compliance managers, security managers, internal auditors; auditors – external and technical auditors; and component owners).

The methodology we followed, and the corresponding results derived are depicted in Figure 1. First, we conducted an interactive interview session at the first face-to-face general assembly in Bilbao, in March 2024. The aim was to get insights about the pilot partners, their pain points and needs during setting-up and conducting audit processes. The results are presented in Section 3. Then we performed semi-structured interviews with the target users, including auditors, compliance managers, and security managers from the different pilot partners and external auditors, which were followed by doing online focus groups. This activity resulted in simple processes for all involved partners. We did a second review round in form of process workshops after we had transformed all simple processes into workflow representations. Then, we developed a general blueprint that is valid for all pilots. The simple processes as well as the workflow representations are presented in Section 4. After the first round of interviews and focus groups, we conducted several online workshops in June 2024 and September 2024 for the development of personas, scenarios and user journeys. In Section 5, we present the final set of personas and scenarios (the user journeys are presented in D4.3 [8] and D4.4 (M24). From all collected insights of the activities, we developed a set of 25 UI/UX requirements for developing the EMERALD UI, which are presented in Section 6.

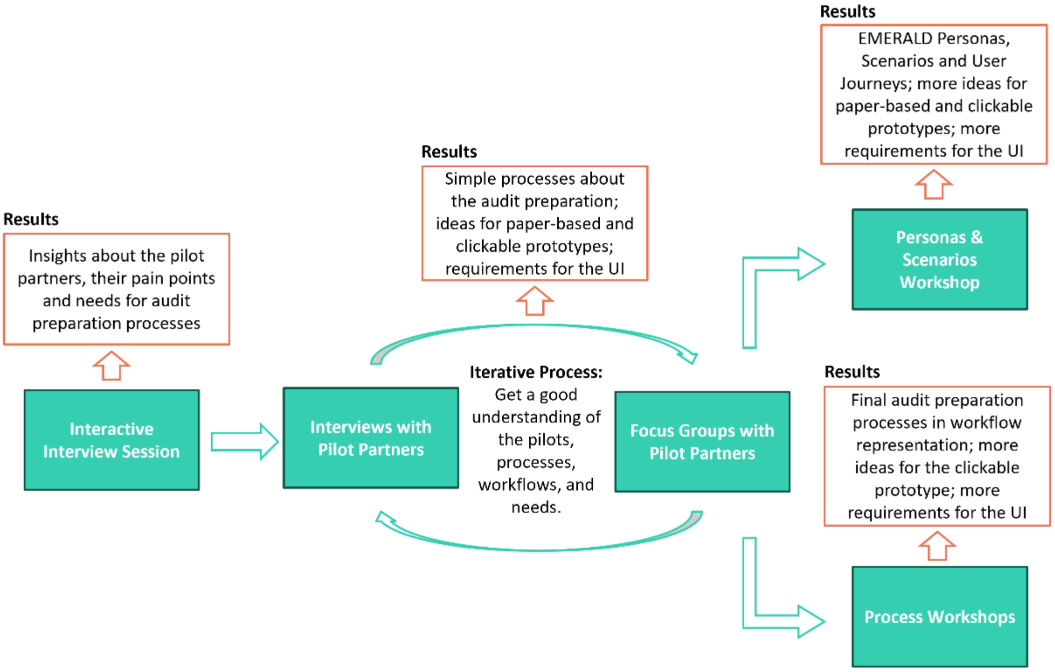

Results
Insights about the pilot partners, their pain points and needs for audit preparation processes
Interactive Interview Session
Interviews with Pilot Partners
Results
Simple processes about the audit preparation; ideas for paper-based and clickable prototypes; requirements for the UI
Iterative Process:
Get a good understanding of the pilots, processes, workflows, and needs.
Focus Groups with Pilot Partners
Results
EMERALD Personas, Scenarios and User Journeys; more ideas for paper-based and clickable prototypes; more requirements for the UI
Personas & Scenarios Workshop
Results
Final audit preparation processes in workflow representation; more ideas for the clickable prototype; more requirements for the UI
Process Workshops

Figure 1. Overall methodology applied in WP4

2.1 Interactive Interview Session

The interactive interview session was conducted at the general assembly in Bilbao, in March 2024. The goal of this session was to get insights about the pilot partners, their pain points, and their needs during setting-up and conducting audit processes, as well as to get first ideas or insights on where the EMERALD UI could support them. A set of six questions was prepared:

- Q1: How do the current audit preparation processes look like for your pilot?
- Q2: What are the “pain points” for your current audit process?
- Q3: Are there any specific tasks to be solved by EMERALD?
- Q4: How can EMERALD help mitigate these “pain points”? Expectations?
- Q5: What tools are you currently using for the audits in your pilot?
- Q6: Which certification schemes are you as pilot interested in?

Procedure

This interview session was conducted in the whole plenum of the general assembly in Bilbao. At the beginning of the interview session, the idea of the session was introduced to the whole consortium. After all pilot partners agreed to participate, they were asked to answer the above questions one after the other. Additionally, all EMERALD partners in the meeting had the opportunity to ask further questions of interest.

The interactive interview session was recorded, later on transcribed, and qualitatively analysed. The results of this session can be found in Section 3.

2.2 Interviews

The overall goal of the interviews was twofold: First, with the interviews we aimed to get a deeper understanding of how the audit preparation processes of the pilot partners and the audit processes of the external auditors (NIXU/DNV) took place. In the context of EMERALD [2], the target groups are, on the one hand, the pilot partners, and particularly those employees who are responsible for preparing and ensuring compliance with cybersecurity standards in the respective organisations. These employees consist of (internal) auditors, chief information security managers, compliance managers, security managers, etc. The second target group is (external) auditors, i.e., auditors who are assigned to conduct the cybersecurity audits within the scope of an official audit. Second, the interviews helped us to elicit requirements for the development of the EMERALD UI/UX.

In more detail, the goal of the interviews is to elicit in-depth insights about the work of auditors, compliance managers (CM), and (chief information) security managers in relation to continuous cloud auditing processes. With the interviews we aimed to get: i) a good understanding of the work of our target users in general, ii) activities and tasks relevant to the certification process of cloud computing systems, iii) insights on how EMERALD could support these working activities, iv) insights about the target users' expectations regarding the EMERALD UI, v) insights about existing pain points, and vi) information about the users' background knowledge, especially regarding artificial intelligence (AI) (as some parts of EMERALD will use AI technologies). By analysing the given answers, we were able to elicit a first set of UI requirements.

Accordingly, we prepared an interview guideline covering the following topics: i) questions to obtain general information about the participants, including their background (education) and their role in the company including the respective activities, ii) questions about the workflows for the audit preparation, iii) questions about how EMERALD could support them, and iv) questions about AI in general and AI literacy in specific. To comply with the current GDPR, we also prepared an information sheet for participants, which provided interviewees with all relevant information about the interview, including the data protection. We also prepared a consent form that allowed us to obtain the written consent from the participants to use the interview results. In addition, we provided a data protection information sheet. All prepared documents can be found in *APPENDIX A: Interview Documents* and were also added to the EMERALD D7.2 deliverable [9].

Procedure

To invite our respective target groups, we contacted the EMERALD pilot partners and the external auditors and asked them to bring us in contact with their (internal) auditors, compliance managers and information security managers. We scheduled an interview appointment with all interviewees. In advance, we sent them the participant information sheet and the data protection sheet and gave them the possibility to clarify any open questions. We then asked them to sign the consent form and send it back to us.

All but one of the interviews were conducted via MS Teams, recorded, and later transcribed. One of the interviews was conducted offline – meaning that CaixaBank received the interview guideline from us and collected the answers from their Information Security Governance team in a written way.

The primary interview data was analysed through qualitative content analysis, following Glaeser and Laudel [10]. The basic procedure consists of understanding and interpreting the collected texts (interview transcripts) in a systematic and rule-based way. The aim of this analysis is to uncover the workflows and processes on how to prepare for an audit, existing pain points, how the EMERALD UI might help, and to derive concrete requirements for the EMERALD UI/UX development. The results were condensed into one slide set per pilot partner. These slide sets were sent out to the respective partners in preparation for the planned focus groups (see Section 2.3).

Altogether, we have conducted 8 interviews in the timespan of March 2024 to February 2025 with compliance managers, security managers and auditors, as depicted in Table 2.

Table 2. Overview of the conducted interviews

Pilot Partners	Participants	Type
IONOS	- 1 interview with a leader of the security management team	Online in MS Teams
	- 1 interview with a security manager	Online in MS Teams
CloudFerro	- 1 Interview with a compliance manager	Online in MS Teams
	- 1 Interview with a security manager	Online in MS Teams
Fabasoft	- 1 Interview with 3 compliance managers	Online in MS Teams
CaixaBank	- 1 (written) interview with the information security governance team	Written interview answers
NIXU/DNV	- 1 Interview with 3 auditors	Online in MS Teams
	- 1 interview with a compliance manager	Online in MS Teams

2.3 Focus Groups & Process Workshops

To complement the interviews, we held a focus group per pilot, where all interviewees or partners from the respective pilot or external auditors from NIXU/DNV participated in, allowing for an in-depth discussion on the derived results and clarification of any possible misunderstandings.

Focus groups can typically be seen as group interviews but guided by specific triggers for discussion [11]. In our case, the triggers were the consolidated results of the individual interviews, which consisted of a summary of the general insights gained from the interactive interview session of the general assembly in Bilbao (March 2024), the processes derived from the individual interviews, and our interpretation of where the EMERALD UI could offer support. These processes were presented in a simple process format.

In the next step, we further improved and enhanced the elicited processes. First, we transferred the simple processes into workflow representations – one covering the status quo and one covering the status of how the process would look like with the EMERALD UI. Then, we set up a series of process workshops with all pilot partners and the external auditors to perform another review round on the processes. Finally, we were able to derive a blueprint process serving as an overall EMERALD process for all pilot partners.

Procedure

To set up a focus group, we contacted the pilot partners and the interview participants via email. In this email, we invited the participants to an online focus group and attached the corresponding slide set with our interview findings. Additionally, the participants were asked to go through the slide set before the focus group was scheduled to ensure they could provide us with valuable feedback and additional details beyond the already collected data.

During the focus group, we guided the participants through the prepared slide set and asked for concrete input and feedback. This time, the discussion was not recorded, but notes were taken. After the focus group, the slide set with the processes was adapted with all gained insights and sent out again to the respective focus group participants.

We have conducted 4 focus groups as depicted in Table 3. The explicit focus group with IONOS was omitted (as it took some time to do the second interview) and instead combined with the final workshop for the process validation.

Table 3. Overview of the conducted focus groups and process workshops

Pilot	Participants	Type
CloudFerro	• 1 focus group with the consortium member	Online in MS Teams
	• 1 process workshop with the consortium member	Online in MS Teams
Fabasoft	• 1 focus group with 1 compliance manager and 1 consortium member	Online in MS Teams
	• 2 process workshops with the consortium members	Online in MS Teams
CaixaBank	• 1 focus group with the pilot partners	Online in MS Teams
	• 1 process workshop with the consortium member	Online in MS Teams
DNV/NIXU	• 1 focus group with 1 compliance manager and the NIXU/DNV project manager from the consortium	Online in MS Teams
	• 2 process workshops with the consortium members, an external auditor and a compliance manager	Online in MS Teams

In the next step, we further improved and enhanced the first elicited simple processes. For each pilot partner and the auditors, we transferred the manual process, and the process enhanced with the EMERALD solution into the two respective workflow representations. As a result, we created for each pilot partner and the auditors an individual Miro[4] board, where we included both processes. Additionally, we added a first version of the blueprint, where we tried to combine all different processes into one that should be valid for all pilot partners. Afterwards, we sent the pilot partners and the auditors an email with the link to the boards and asked them to go through the processes and gather feedback.

We set up individual process workshops (February/March 2025) with the pilot partners and auditors, as presented in Table 3, where we went through the processes together to see what to improve, we integrated the collected feedback and adapted the processes accordingly. Additionally, we asked all invited parties to have a final look at the processes to confirm that they were ok for them. These activities resulted in the final definition of the processes for the pilot partners and the auditors: the current "as-is" process, and the process with EMERALD support. Additionally, a blueprint process that is valid for all pilot partners was created. This blueprint could be of interest for other companies who would like to use the EMERALD solution to support their audit preparation processes. The final processes per pilot partner and auditors, and the blueprint are presented in Section 4.

2.4 Personas & Scenarios Workshops

Based on the insights gained from the interviews and the focus groups, e.g., what the audit preparation processes and audits in general look like, which persons and roles are involved in these processes and what information is needed, a first *Personas and Scenarios* workshop was organised. The goal of this workshop was to develop detailed personas and scenarios on how the target groups will use the EMERALD UI and which functionalities should be available.

Personas are a goal-directed design tool introduced by Cooper [12]. A persona typically represents a fictional individual or a representative group of persons with similar characteristics (see [13], [14]). They are often described in a narrative way to make the person seem authentic and to provide the needs of these individuals in the related context [15]. Personas are typically

[4] https://miro.com/

used in combination with scenarios. Scenarios describe, in a narrative way, how target users will ideally interact with the developed technology [16]. After developing personas and scenarios, user journeys [17] are another design method to help understand the interaction between a user and a technology. The initial user journeys have been presented in D4.3 [8] and the final user journeys will be presented in D4.4 (M24).

Overall, defining personas and engaging in scenarios helps to gain a deeper understanding of the users, their tasks, and their interactions with the system. The results of the workshops should tailor the UI/UX of EMERALD to the specific needs of the users (e.g., compliance managers and auditors). The aim is to clarify how the different user groups will interact with the EMERALD UI during different working activities and tasks. Furthermore, this will help gathering information on the functionalities to be provided in the EMERALD UI.

Altogether, we have conducted four workshops based on the insights gained from the interviews and focus groups, as presented in Table 4. In the two workshops held in June 2024, we were able to derive four personas and three scenarios. As the development of the personas and scenarios was not completed, we set up again two other workshops in autumn 2024. One workshop with NIXU/DNV to create auditor-specific personas and scenarios, and another with the EMERALD consortium partners to finalize and expand existing work. Finally, we developed seven personas across three stakeholder groups and 16 scenarios.

Table 4. Overview of all Persona and Scenario Workshops

Personas & Scenario Workshop	Date	Type	Workshop Results
Personas & Scenarios Workshop Part I	05.06.2024	Online in MS Teams	Development of 4 Personas: Emerson, Riley, Dylan, Charlie
Personas & Scenarios Workshop Part II	12.06.2024	Online in MS Teams	Development of 3 Scenarios for Emerson, Dylan, Charlie
Personas & Scenarios Workshop with NIXU/DNV	13.08.2024	Online in MS Teams	Development of 2 Personas and 2 Scenarios for Jarkko and Eero
Personas & Scenarios Workshop Part III	07.10.2024	Online in MS Teams	Development of 1 additional Persona, Morgan, and all missing scenarios

Once all the relevant personas and scenarios were elaborated and well defined, we derived from them the so-called “personas-on-the-go”. “Personas-on-the-go” provide a very concise, precise summary of our personas, highlighting key characteristics in a brief description. These ensure that target users and external audiences can quickly understand the purpose and needs of the personas in relation to the EMERALD UI. All personas, the respective scenarios and the “personas-on-the-go” are presented in Section 5.

Procedure

To invite participants to the workshop, we contacted the pilot partners and all members of WP4 and WP5 by email. All Personas & Scenarios Workshops were conducted online using MS Teams. To facilitate collaboration, we used Miro, an online collaborative whiteboard.

Below, we describe all Persona & Scenarios Workshops done in more detail:

Workshop Part I: The first part of the workshop was attended by 11-14 participants. The agenda was as follows: first, we introduced how to use the Miro Board. Then, we set the stage and goal of the workshop and invited the participants to take part in an activity, namely, to note down their expectations towards the workshop shortly. Afterwards, we presented a summary of the work processes elicited from the different pilot partners' interviews. Having this information in mind (and on the Miro board), we divided the participants into four groups. Each group was asked to create a persona, using a predefined persona template, representing one of the target-users of the EMERALD Project.

The persona template consisted of three parts with several sub-topics:

- About the persona: This part includes private information, occupation, goal, and other characteristics.
- What do I do: This section collects working tasks, motivation and goals at work, frustrations and pain points.
- Contacts: Information about departments and roles the persona is working with.
- Work context: This covers information about day-to-day tasks, and where the EMERALD UI could help.

Workshop Part II: The second part of the workshop was attended by eleven participants. The agenda was as follows: first, we made a short recap of the first part of the workshop by briefly summarizing the four personas developed. Second, we introduced scenarios and user stories as co-design method in general. Then, we presented 6 pre-defined scenarios as starting points. Afterwards, we divided the participants into three groups and asked them to create a scenario for the persona they had developed in the first workshop. They could use one of the pre-defined scenarios as a starting point. After developing the scenario, they were asked to break it down into different steps to determine how the persona would interact with the EMERALD UI and to discuss these user stories in relation to the pre-defined mock-ups.

The activities of both workshops resulted in four personas: Emerson – Compliance Manager in Financial Services, Riley – Cloud Provider Compliance Manager, Dylan – Internal Control Owner, Charlie – Internal Auditor, and three scenarios: Scenario 1: Emerson – Bring your own certification scheme, Scenario 2: Dylan – ICO Requirement Implementation and Scenario 3: Charlie – Preparation of an audit by an internal auditor.

Persona & Scenario Workshop with NIXU/DNV: The Workshop with NIXU/DNV was held in August 2024. This workshop was conducted online in MS Teams, and we used Miro again to facilitate the collaboration.

Before the workshop, we enhanced the already existing EMERALD Miro board to develop auditor personas. We held a short meeting with the colleagues from NIXU/DNV and explained what we would like to have and how to use the Miro Board. We also explained the two templates we had prepared for the development of personas and scenarios that we used in the previous workshops. Subsequently, we asked them to develop necessary personas and define respective scenarios for each persona themselves. Afterwards, we held a workshop to go through the personas and the respective scenarios and to discuss and refine them in detail. These activities resulted in two new personas – Jarkko – Lead auditor in a consulting company and Eero – Technical auditor in a consulting company.

Final Personas & Scenarios Workshop Part III: The final workshop was attended by twelve participants. Before inviting all EMERALD partners to the third persona & scenario workshop, we read D5.1 – Pilot definition, set-up & validation plan [18]. The goal was to investigate which additional stakeholders were involved within the pilot definitions and set-up (see D5.1 [18], Section 2). We created a table with all involved stakeholders mentioned in the pilot definitions and discussed with the consortium which of them are relevant for EMERALD. Subsequently, we agreed on a list representing all EMERALD stakeholders and identified, which of them are still missing. This served as a starting point for the final workshop where we prepared a Miro board with a structured template. We highlighted the still missing gaps regarding one persona, several scenarios and user journeys. The corresponding templates were documented in D4.1 [1] – Figure 2 and D4.3 [8], Figure 2.

Table 5 reflects the final status upon completion of all workshops. Additionally, we developed a first set of user journeys for the respective personas which will be presented in *D4.4 – User Interaction and User Experience Concept – v2* (M24). These user journeys are closely tied to the scenarios and the ongoing development of the EMERALD UI and are therefore under continuously development.

Table 5. Status Overview of the Development of Personas, Scenarios and User Journeys

	Roles	Notes	Personas	Scenarios	User Journeys
Compliance Stakeholders	Compliance Manager	UI/UX: they will be merged in one role in the EMERALD UI	Riley	done	in progress
	Compliance Manager for financial services		Emerson	done	in progress
	Internal Control Owner	-	Dylan	done	in progress
Technical Stakeholder	Technical Implementer	One role covering all technical roles including the metric implementer, developers, etc. (Old name: Metric Implementor)	Morgan	done	in progress
Auditor Stakeholders	Internal Auditor	-	Charlie	done	in progress
	External Lead Auditor	UI/UX: they will be merged in one role in the EMERALD UI	Jarkko	done	in progress
	External Technical Auditor		Eero	done	in progress

Gender-bias in Personas and Scenarios

It is known from literature that gender bias during technology development is a problem because women are often under-represented in design teams and in co-creation and co-design processes (see [19], [20], [21]). With regard to personas, several strategies on how to mitigate gender bias during the development of personas and scenarios exist – one of them is to use gender-neutral personas (see [22], [23]) and to formulate scenarios in a gender-neutral way. Therefore, we created a list of gender-neutral names to use during the workshops, and did not ask for a specific gender in the persona template. Afterwards, all gender-specific formulations were removed (e.g., all wording referring to he/she was replaced with they).

To make the development of the personas more fun for the participants, we asked them to create a profile picture for each persona. Originally, we planned to remove the profile pictures from the final personas. However, instead of removing the profile pictures, we made them gender-neutral for several reasons.

- **Inclusivity**: Gender-neutral personas ensure that all users, regardless of gender identity, feel represented and considered in design and decision-making processes [23].
- **Avoiding Bias:** Gendered personas can reinforce stereotypes, such as associating certain roles or behaviours with specific genders. Neutral figures help prevent these biases.

- **Flexibility:** Gender-neutral personas can be more universally applicable, allowing stakeholders to focus on user needs, behaviours, and challenges rather than gender-based assumptions [23].
- **Encouraging Diversity:** They foster a more diverse and equitable approach to problem-solving, ensuring that solutions do not unintentionally exclude or disadvantage any group [23].
- **Reflecting Reality:** Many real-world scenarios involve individuals whose gender is not immediately relevant or who identify outside the binary. Gender-neutral personas acknowledge this diversity [24].

Using gender-neutral profile pictures makes personas and scenarios more inclusive, adaptable, and effective in addressing a broad range of users' needs. Therefore, we decided to keep the profile pictures.

3 Results of the Interactive Interview Session

The interactive interview session was conducted per pilot at the general assembly in Bilbao (March 2024). The results are presented below as follows: first, for each question a short summary is presented, followed by a table summarizing the results of all pilots in more detail.

Q1: How do the current audit preparation processes look like for your pilot?

All pilot partners described the audit preparation processes very similarly. Audits take place yearly up to every 4-5 years. The frequency of the audit depends on the type of the audit (e.g., some audits take place yearly, some only every 2-3 years) and the standard that is audited. Typically, the preparation of an audit is a repetitive and time-consuming manual process that involves many people from different departments, as described in Table 6.

Table 6. Answers given to Q1:
"How do the current audit preparation processes look like for your pilot?"

Q1: How do the current audit preparation processes look like for your pilot?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• repetitive manual processes • involvement of various teams • rely on external consultancy companies • based on a spreadsheet → turned into tickets • documents such as employee certifications, need to be formalized and presented	• multiple audits yearly • time-consuming • audits last 2-4 days • significant preparation time • manual preparation of procedures, policies, and documentation	• traditional audits: not always able to deal with automatically collected evidence or digital support of the steps • automatically collected pre-processed evidence has to be presented as manual evidence • auditors are able to have the evidence chains • many people involved in preparing the audit and during the audit • major tool: spreadsheet • create a huge number of tickets and issues that need to be addressed by a lot of people	• pilot covers several environments • continuous assessment on own premises • internal audit yearly, with additional audits for cloud provider license renewals • periodic audits by ECB every 4-5 years, covering all aspects of bank security • audits occur annually

Q2: What are the "pain points" for your current audit process?

The pilot partners mentioned similar "pain points" that they must deal with during the audit preparation phase, as presented in Table 7. Pain points mentioned are that i) the audit preparation phase is a very costly process as it involves consultancy from outside, and many people and departments from inside, ii) it is a very time-consuming process to show evidence for all requirements necessary for the respective audit, and iii) it needs manual verification of extensive documents.

Table 7. Summary of answers given to the question Q2: "What are the "pain points" for your current audit process?"

Q2: What are the "pain points" for your current audit process?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• costly processes (because of consultancy and manual work) • large workload (because process is based on a spreadsheet which is then turned into tickets manually)	• audits comprehensive & time-consuming • manual verification of extensive documentation • involvement of multiple teams	• many people involved for a huge number of days for one single certification • based on a spreadsheet	• obtaining all evidence • evaluating against internal spreadsheet • need for exhaustive monitoring of critical providers • improving controls, benchmarks, and standards for cloud providers • identifying and implementing required controls for different clouds

Q3: Are there any specific tasks to be solved by EMERALD?

The pilot partners had concrete suggestions for specific tasks to be solved within the EMERALD project and especially by the EMERALD UI, as presented in Table 8. The pilot partners came up with suggestions such as i) automating the collection and identification of relevant documents to show evidence regarding requirements, ii) supporting the whole workflow management, especially including the manual processes, and iii) allowing the automatic extraction of evidence from different documents (for organisational and technical requirements likewise). A direct quote was, furthermore, "*We would like to get rid of our* [spreadsheet]*!*".

Table 8. Summary of answers given to the question Q3: "Are there any specific tasks to be solved by EMERALD?"

Q3: Are there any specific tasks to be solved by EMERALD?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• automate collecting and identifying documentation (e.g., on employee certifications and trainings) • facilitate and automate manual processes	• policy and procedure documentation management, integration of AMOE	• support the whole workflow management including a fair coverage of manual processes • show path for new approach to audits	• real-time monitoring and evidence collection for cloud and on-premises setups • analysis and matching of policies and procedures to certification scheme • need for automated system to recognize documents and controls • linking evidence to source documents for audit purposes • providing extracted evidence from commercial tools for assessment • writing wrapper for tools to submit evidence • include on-premises assessment if desired

			• building internal tool similar to Clouditor[5] for automating evidence collection from different environments

Q4: How can EMERALD help mitigate these “pain points”? Expectations?

To mitigate the existing pain points, the pilot partners have several ideas where the EMERALD project might come into play, as described in Table 9. For example, EMERALD could help to i) reduce the manual work of evidence collection, ii) support the verification process of evidence in relation to requirements, iii) reduce the involved personnel costs as it reduces the time for preparing the audits and the number of persons involved across the companies, and iv) if possible, the solution developed within EMERALD should be accepted by auditors as a tool supporting the audit process.

Table 9. Summary of answers given to the question Q4:
“How can EMERALD help mitigate these “pain points”? Expectations?”

Q4: How can EMERALD help mitigate these “pain points”? Expectations?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• collect, identify and present important documentation • automate repetitive processes → reduce manual work	• automate the verification process • main expectation: costs of the audits will be decreased	• assist throughout all respective manual processes regarding organizational parts and evidence • map EUCS into the digital world • not only collect and manage these things digitally and automatically, but also enable complete audit chains • assist with a transition into a new approach for audits • technical audit API to standardize the communication of evidence for technical requirements • EMERALD solution should be accepted by auditors	• comparing internal tool with Clouditor for auditing • compare our own tool with EMERALD/ Clouditor and see how they can complement each other • integrate metrics recommender and AMOE into audit processes • deploy and utilize selected EMERALD tools for real-time assessments

Q5: What tools are you currently using for the audits in your pilot?

So far, the pilot partners use different tools for preparing an audit, as shown in Table 10. Nearly all partners use a spreadsheet to manage the requirements of the respective standards. One row represents one concrete requirement. For each single requirement, each row contains information about how the respective requirement is fulfilled (including links to the respective

[5] https://github.com/clouditor/clouditor

documents and evidence), who is responsible for the requirement and what the status for the requirement is. Additionally, the pilot partners use other tools for managing the requirements such as JIRA, OpenStack or other dashboards or tools tailored to their needs.

Table 10. Summary of answers given to the question Q5: "What tools are you currently using for the audits in your pilot?"

Q5: What tools are you currently using for the audits in your pilot?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• Spreadsheet • JIRA	• Mostly manual • OpenStack • Spreadsheet/Word	• Spreadsheet • Predefined Workflows and tickets • Internal monitoring tool	• Center for Internet Security benchmarks for cloud environments • Own centralized tool is planned with dashboard

Q6: Which certification schemes are you as pilot interested in?

Table 11 presents the certifications standards in which the pilot partners are interested and which of them they would like to be supported by EMERALD. Most of the pilot partners are interested in BSI C5 and EUCS schemes, as well as other standards relevant to their individual cloud services.

Table 11. Summary of answers given to the question Q6: "Which certification schemes are you as pilot interested in?"

Q6: Which certification schemes are you as pilot interested in?			
Pilot 1: IONOS	**Pilot 2: CloudFerro**	**Pilot 3: Fabasoft**	**Pilot 4: CaixaBank**
• BSI C5	• ISO • BSI C5	• EUCS • BSI C5 • AIC4	• ENS • DORA • Requirements from European Central Bank • Internal schemes

4 Work Processes

This section presents the final version of the elicited work processes in a workflow representation derived from the interviews, focus groups, and workshops with all pilot partners and with NIXU/DNV. For each pilot partner, and auditors and compliance managers from NIXU/DNV, we present first the "as-is" processes followed by the enhanced processes when using the EMERALD solution. Finally, we present a blueprint process which is valid for all pilot partners.

Goal: The goal of the elicitation of the work processes is fourfold: First, these processes are necessary for us to understand which tasks the pilot partners or the compliance managers from NIXU/DNV need to do to prepare for an audit; additionally, we need to know how auditors perform an audit. Second, these processes help us to design the EMERALD UI in that we get to know which functionality the UI should be provided to support the pilot partners, compliance managers and auditors likewise. Third, the development of the processes helped us to elicit concrete (design) requirements for the EMERALD UI. Finally, combining all processes into a blueprint may be valuable for other companies seeking to use the EMERALD solution to enhance their audit preparation processes or to support audit executions.

Preparing for or conducting an audit for cloud service providers is a very sensitive and challenging task that must ensure data protection throughout the entire process. Additionally, all pilot partners and NIXU/DNV perform the audit preparation or conduct an audit very similarly but have at the same time individual company-specific procedures and strategies to do so. All processes described below, are kept as general as possible so as not to provide any sensitive or sensible data from the pilot partners or NIXU/DNV.

Remark: During the course of the project, the wording regarding the certification schemes and their corresponding requirements was changed to controls. Additionally, the term "certification target" was changed to "target of evaluation". Subsequently, these wordings were taken over for all processes – in the text and the related figures.

4.1 Work Processes in Workflow Representation

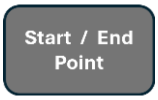
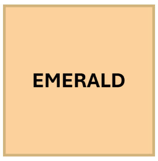
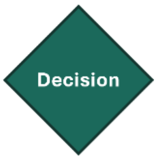
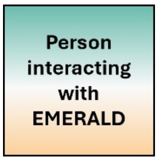
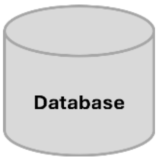
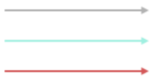
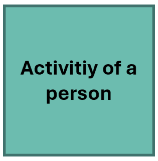
In D4.1 [1], we presented the first elicited work processes in a very simple way and only for some (not all) pilot partners and NIXU/DNV. We presented the process along the major steps that are necessary for conducting an audit preparation or in the context of an audit for conducting the audit.

In D4.2, we have used the simple processes from D4.1 and developed them for all pilot partners and NIXU/DNV. In the following we provide for each step in the process a short description of the respective tasks (see Figure 2, Figure 6, Figure 10, Figure 14, Figure 18, Figure 22). Subsequently, we present how each step and the corresponding tasks could be supported by the EMERALD solution (see Figure 4, Figure 8 ,Figure 12, Figure 16, Figure 20, Figure 24). Please note that EMERALD's support for the simple processes were only first ideas, as the development of the EMERALD UI was just at the beginning.

Based on these simple processes, we created concrete workflow representations for all pilot partners and NIXU/DNV and transferred the simple process into a workflow representation. First, we present the workflow representation of how the audit preparation process is currently done (see Figure 3, Figure 7, Figure 11, Figure 15, Figure 19, Figure 23). Second, we present the workflow representation of how this process can be carried out using the EMERALD UI (see Figure 5, Figure 9, Figure 13, Figure 17, Figure 21, Figure 25).

Table 12 presents all shapes used in the workflow representation and the corresponding description of what each shape stands for. Be aware that EMERALD's support in the workflow representations is developed in line with the current status of the EMERALD UI regarding the available functionalities and features.

Table 12. Presentation of all shapes used in the workflow representation of the audit preparation processes

Shape/Symbol	Function	Shape/Symbol	Function
	The rectangle with round corners defines the start and end point of a process.		A rectangle in orange represents a process step conducted by EMERALD.
	A diamond represents a decision in the process.		A rectangle in green and oranges represents a process step conducted by a person using EMERALD.
	The cylinder represents an input or output from and to a database.		A line is a connector that shows the relationships between the representative shapes of the process. Grey lines are normal connectors, green lines represent an "ok" decision, and red lines represent a "not ok" decision.
	A rectangle in green represents a process step conducted by a person.		

4.2 Work Processes of Compliance and Security Managers per Pilot Partner

This section describes the results of the interviews, focus groups and workshops conducted with all pilot partners. First, we present the derived audit preparation processes in a simple process representation. Second, we transfer the simple process representation into a detailed workflow representation. Then, we present how these processes – the simple process representation and the workflow representation-, would look like when being supported by the EMERALD solution.

In the following, we present the work processes elicited from Pilot 1: IONOS, Pilot 2: CloudFerro, Pilot 3: Fabasoft, Pilot 4: CXB and the processes derived for auditors and compliance managers supported by NIXU/DNV.

For Pilot 1, Pilot 2 and Pilot 3 these processes refer to how they perform the audit preparations within their companies for their own cloud services. This is also the case for the processes of the compliance manager from NIXU/DNV.

In Pilot 4, the general setting is a bit different from the other pilots. CXB is a Spanish bank that holds many on-premises services from different SaaS or IaaS providers. Additionally, due to regulation in the financial domain, there is a need for continuous compliance in services not hosted by CXB themselves. Therefore, the audit preparation process for this use case deals with how CXB manages this process regarding cloud service providers and the usage of their services.

Finally, for the NIXU/DNV auditors, the processes are elicited from the perspective of performing an external audit of a cloud service provider.

4.2.1 Pilot 1: IONOS

We conducted two interviews with IONOS employees: one with the head of the security management team and one with a team lead security manager. Due to time scheduling issues the focus group was omitted. Instead, the workshops to discuss the simple processes and the workflow representation were done together. The simple process of how to prepare for an audit was derived. Figure 2 presents the simple processes without EMERALD support and Figure 4 presents the simple process with EMERALD support.

After having transformed the simple process representation into a workflow representation, we conducted a workshop with IONOS colleagues to validate the processes. Figure 3 presents the derived workflow representation of the simple process as it is now, and Figure 5 presents the workflow representation with EMERALD support.

4.2.1.1 Simple Process without EMERALD support

The simple process without EMERALD support consists of the following four phases:

- **Phase 1 – Preparation** (Figure 2, Phase 1): In the first step, the compliance manager prepares the system landscape. Additionally, for the audit preparation, the internal change management checks whether the controls have been changed or updated.
- **Phase 2 – Documentation** (Figure 2, Phase 2): In the second step, the compliance manager needs to ensure that all mandatory documents and the system descriptions are up to date.
- **Phase 3 – Management of Controls** (Figure 2, Phase 3): The CM implements the controls extracted from the security policies and sets up a control matrix (spreadsheet) for managing the controls. The spreadsheet consists of information such as: controls; control frequency; type of control; responsible person for the control; evidence we need to show that it has been implemented.
- **Phase 4 – Audit Scope** (Figure 2, Phase 4): In this phase the audit scope description needs to be kept up to date for preparing the audit.
- **Phase 5 – Audit Setup** (Figure 2, Phase 5): In this phase, the audit is conducted with a notified body. They decide for the audit team (external), and they need to update the contract. If the audit is against BSI C5, there needs to be a certificate confirming no conflicts of interest (both sides). Then the audit dates are set, the audit plan needs to be agreed to and IONOS hands over relevant and up-to-date documents to the auditors, including the spreadsheet with all established controls for BSI C5.

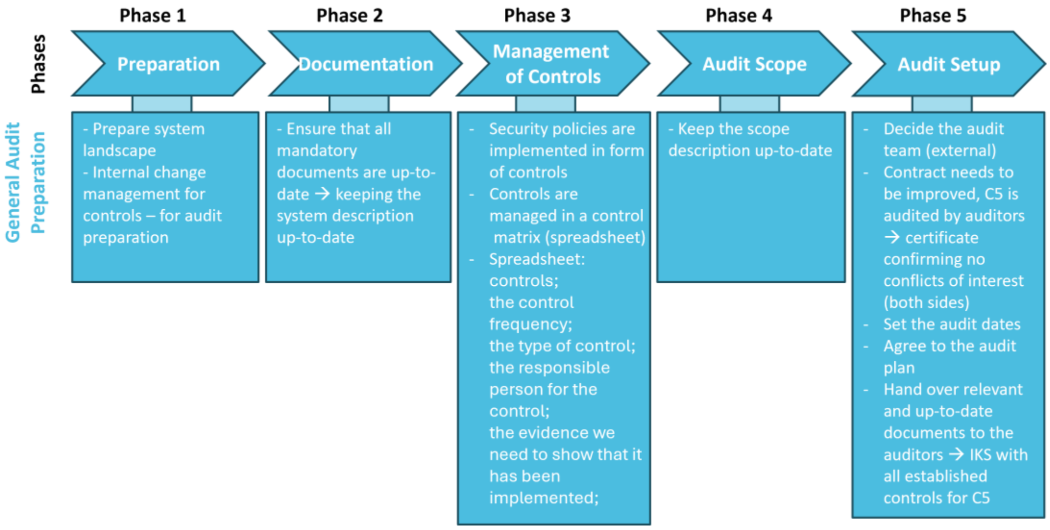

Phases
General Audit Preparation
Phase 1
Preparation
- Prepare system landscape
- Internal change management for controls – for audit preparation
Phase 2
Documentation
- Ensure that all mandatory documents are up-to-date → keeping the system description up-to-date
Phase 3
Management of Controls
- Security policies are implemented in form of controls
- Controls are managed in a control matrix (spreadsheet)
- Spreadsheet: controls; the control frequency; the type of control; the responsible person for the control; the evidence we need to show that it has been implemented;
Phase 4
Audit Scope
- Keep the scope description up-to-date
Phase 5
Audit Setup
- Decide the audit team (external)
- Contract needs to be improved, C5 is audited by auditors → certificate confirming no conflicts of interest (both sides)
- Set the audit dates
- Agree to the audit plan
- Hand over relevant and up-to-date documents to the auditors → IKS with all established controls for C5

Figure 2. IONOS – Simple process representation without EMERALD support

4.2.1.2 Workflow Representation of the Process without EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was discussed with the colleagues from IONOS, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 3.

- **Phase 1 – Preparation** (Figure 3, Phase 1):
  - Landscape preparation: CM prepares the system landscape for setting up the audit preparation process.
  - Change management: CM initiates the change management and uses the established internal control system including a spreadsheet.
- **Phase 2 – Documentation** (Figure 3, Phase 2):
  - Documentation: In the second step, the CM needs to ensure that all mandatory documents as well as the system descriptions are up to date.
- **Phase 3 – Management of Controls** (Figure 3, Phase 3):
  - Security policies and controls: CM organizes all security policies with controls.
  - Spreadsheet creation: CM manages the controls in a spreadsheet. The spreadsheet consists of information such as: controls; control frequency; type of control; responsible person for the control; evidence we need to show that it has been implemented.
- **Phase 4 – Audit Scope** (Figure 3, Phase 4):
  - Audit scope: CM needs to keep the audit scope description up to date.
  - Control checking: CM checks the status of the controls and escalates if the evidence reported is insufficient or not prepared in time.
- **Phase 5 – Audit Setup** (Figure 3, Phase 5):
  - Audit setup: The Event Manager sets up the audit and decides on the audit team (external notified body).
  - Renew contract: After deciding for an audit, the IONOS team updates the contract with the auditors. If the audit is against BSI C5, there needs to be a certificate confirming no conflicts of interest (both sides).
  - Set practicalities: Audit dates, scope and parameters are set and need to be agreed to. Also, the individual audit plan must be agreed to.

- Report creation: Reports must be created: including an internal control system with all established controls and the mapping to BSI C5 criteria.
- Hand over report: Reports must be handed over to the auditors at the beginning of the audit.

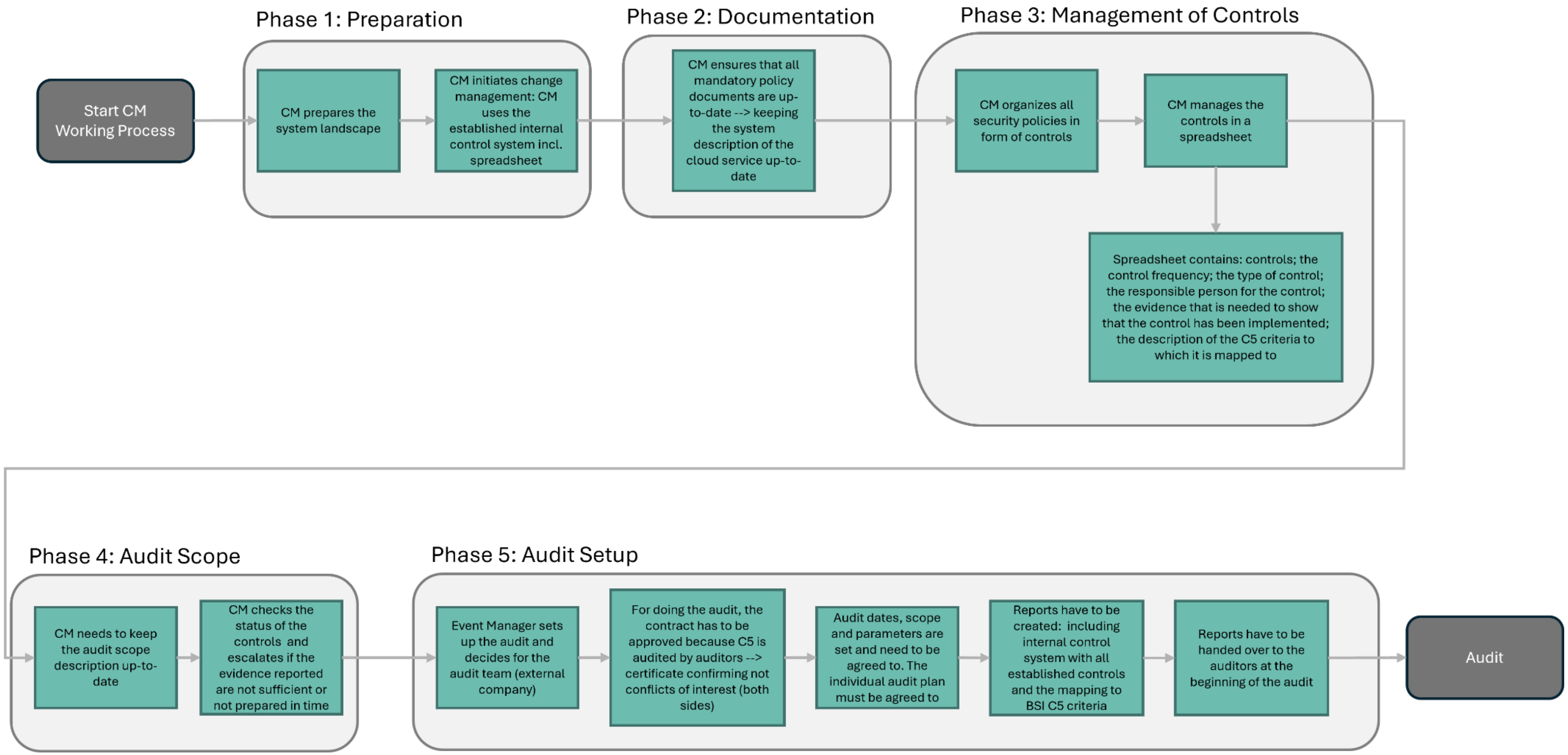

Phase 1: Preparation
Phase 2: Documentation
Phase 3: Management of Controls
Start CM Working Process
CM prepares the system landscape
CM initiates change management: CM uses the established internal control system incl. spreadsheet
CM ensures that all mandatory policy documents are up-to-date --> keeping the system description of the cloud service up-to-date
CM organizes all security policies in form of controls
CM manages the controls in a spreadsheet
Spreadsheet contains: controls; the control frequency; the type of control; the responsible person for the control; the evidence that is needed to show that the control has been implemented; the description of the C5 criteria to which it is mapped to
Phase 4: Audit Scope
Phase 5: Audit Setup
CM needs to keep the audit scope description up-to-date
CM checks the status of the controls and escalates if the evidence reported are not sufficient or not prepared in time
Event Manager sets up the audit and decides for the audit team (external company)
For doing the audit, the contract has to be approved because C5 is audited by auditors --> certificate confirming not conflicts of interest (both sides)
Audit dates, scope and parameters are set and need to be agreed to. The individual audit plan must be agreed to
Reports have to be created: including internal control system with all established controls and the mapping to BSI C5 criteria
Reports have to be handed over to the auditors at the beginning of the audit
Audit

Figure 3. IONOS – Workflow Representation without EMERALD support

4.2.1.3 Simple Process with EMERALD support

For each of the five phases mentioned above in the IONOS audit preparation process, we have derived some ideas on how the audit preparation process of cloud solutions at IONOS could be supported by the EMERALD UI, as shown in Figure 4.

- **Phase 1 – Preparation** (Figure 4, Phase 1):
  - Setup controls: The CM can use EMERALD to support the preparation process by getting the list with all controls.
- **Phase 2 – Documentation** (Figure 4, Phase 2):
  - Upload documents: The CM can upload all relevant and updated documents into the EMERALD UI.
  - Extract evidence: EMERALD can help extract evidence from the documents and map them to the controls.
  - Visualisation of Controls/Metrics and Evidence: EMERALD UI/UX provides a table showing the controls/metrics and the found evidence and links to the respective documents.
- **Phase 3 – Management of Controls** (Figure 4, Phase 3):
  - List of controls: EMERALD provides the list of the controls for the CM.
  - Management of controls: The CM can use EMERALD to manage the controls; assign responsible people to a control; add documentation, and keep track of the evidence; etc.
- **Phase 4 – Audit Scope** (Figure 4, Phase 4): EMERALD can help to keep the audit scope up-to-date.

- **Phase 5 – Audit Setup** (Figure 4, Phase 5):
  - Reporting: EMERALD can support preparing and printing out the reports (e.g., different formats, different content) that need to be handed over to the auditors at the beginning of the audit.

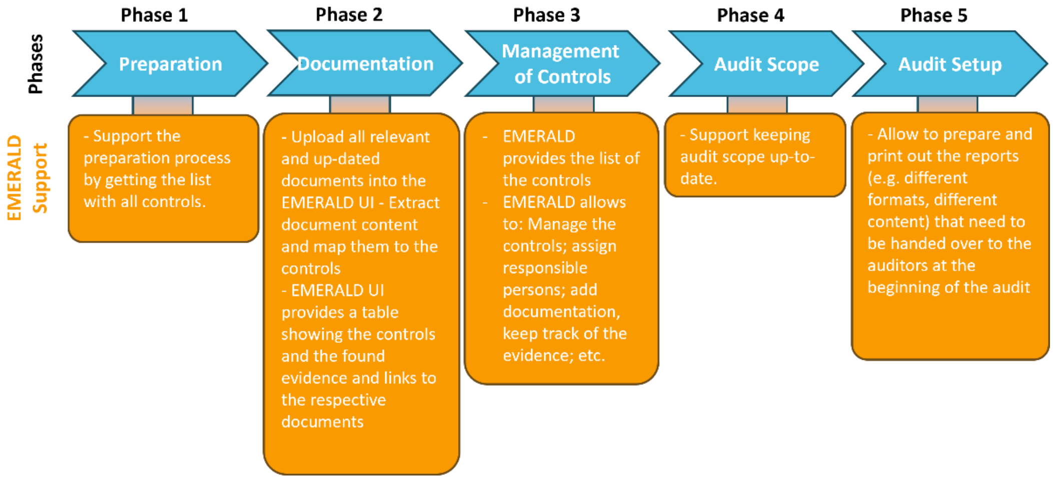

Phases
EMERALD Support
Phase 1
Preparation
- Support the preparation process by getting the list with all controls.
Phase 2
Documentation
- Upload all relevant and up-dated documents into the EMERALD UI - Extract document content and map them to the controls
- EMERALD UI provides a table showing the controls and the found evidence and links to the respective documents
Phase 3
Management of Controls
- EMERALD provides the list of the controls
- EMERALD allows to: Manage the controls; assign responsible persons; add documentation, keep track of the evidence; etc.
Phase 4
Audit Scope
- Support keeping audit scope up-to-date.
Phase 5
Audit Setup
- Allow to prepare and print out the reports (e.g. different formats, different content) that need to be handed over to the auditors at the beginning of the audit

Figure 4. IONOS – Simple process representation with EMERALD support

4.2.1.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from IONOS, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 5.

- **Phase 1 – Preparation** (Figure 5, Phase 1):
    - System landscape preparation: CM prepares the system landscape for the audit.
    - CM initiates change management: CM uses the established internal control system (including spreadsheet) to initiate the change management.
    - Upload Controls: CM uploads the certification scheme, thus the extracted controls, into EMERALD.
    - EMERALD: EMERALD makes all controls available.
    - EMERALD: EMERALD automatically assigns metrics to controls.
- **Phase 2 – Documentation** (Figure 5, Phase 2):
    - Check Metrics: CM goes through all automatically assigned metrics to a control.
    - Metric Check not ok: CM checks all metrics and changes them where needed.
    - Metric Check ok: CM continues in the process.
- **Phase 3 – Management of Controls** (Figure 5, Phase 3):
    - Setup target of evaluation: New target of evaluation needs to be set up and the appropriate evidence extractors need to be installed. There, the CM can upload the policy documents in EMERALD.
    - The CM sets up the audit scope using the created target of evaluation in EMERALD.
    - EMERALD automatically extracts metrics-related data/information from the documents and makes the assessment results available to the CM.
    - Managing Controls: CM can manage all controls in EMERALD.
    - Filtering Controls: CM can filter for all controls that are still marked as "open" and manually check the assessment results.
    - Check for next open Control: If a next open control exists, the CM checks the control and its assessment results / evidence.
    - Check Assessment Result: If the check is ok, based on the available assessment results, CM can set the control / metric in EMERALD to compliant.
    - Check Assessment Result: If the check is not ok, CM/Person assigns control/metric to a person or a department. The person checks the assessment results of the assigned control/metric provided in EMERALD.
    - Check Assessment Result (by Person): If the check is ok based on the available assessment results, the person can set a control/metric to compliant in EMERALD.
    - Check Assessment Result (by Person): If the check is not ok, but the person knows how to solve it, the person implements the metric and sets the metric/control in EMERALD to compliant.
    - In both cases, the person assigns the control/metric back to the CM.
    - All Controls Checked: After the CM has checked all controls/metrics and documents, the CM consolidates everything for the audit.
- **Phase 4 – Audit Scope Management** (Figure 5, Phase 4):
    - Keep Audit Scope Up-to-date: CM needs to keep the audit scope description up-to-date.
    - Check Audit Scope Reporting: CM checks the reporting and escalates if the evidence reported is insufficient or not prepared in time with the help of EMERALD.
- **Phase 5 – Audit Setup** (Figure 5, Phase 5):
    - Setup Audit: The Event Manager sets up the audit and decides for the audit team (external company).
    - Renew Contract: After deciding for an audit team, IONOS needs to update the contract with the auditors. If the audit is against BSI C5, there needs to be a certificate confirming no conflicts of interest (both sides).

- Set Practicalities: Audit dates, scope and parameters are set and need to be agreed upon. Also, the individual audit plan must be agreed to. The decision needs to be made on whether EMERALD can be used during the audit.
- Use EMERALD: If it is agreed to that the audit can be conducted with the support of EMERALD, it can be used to evaluate controls/metrics, assessment results and documents.
- Use EMERALD: If it is not agreed to that the audit can be conducted with the support of EMERALD, all evidence must be handed over to the auditors at the beginning of the audit; this includes the internal control system with all established controls, evidence and the mapping to BSI C5 criteria.

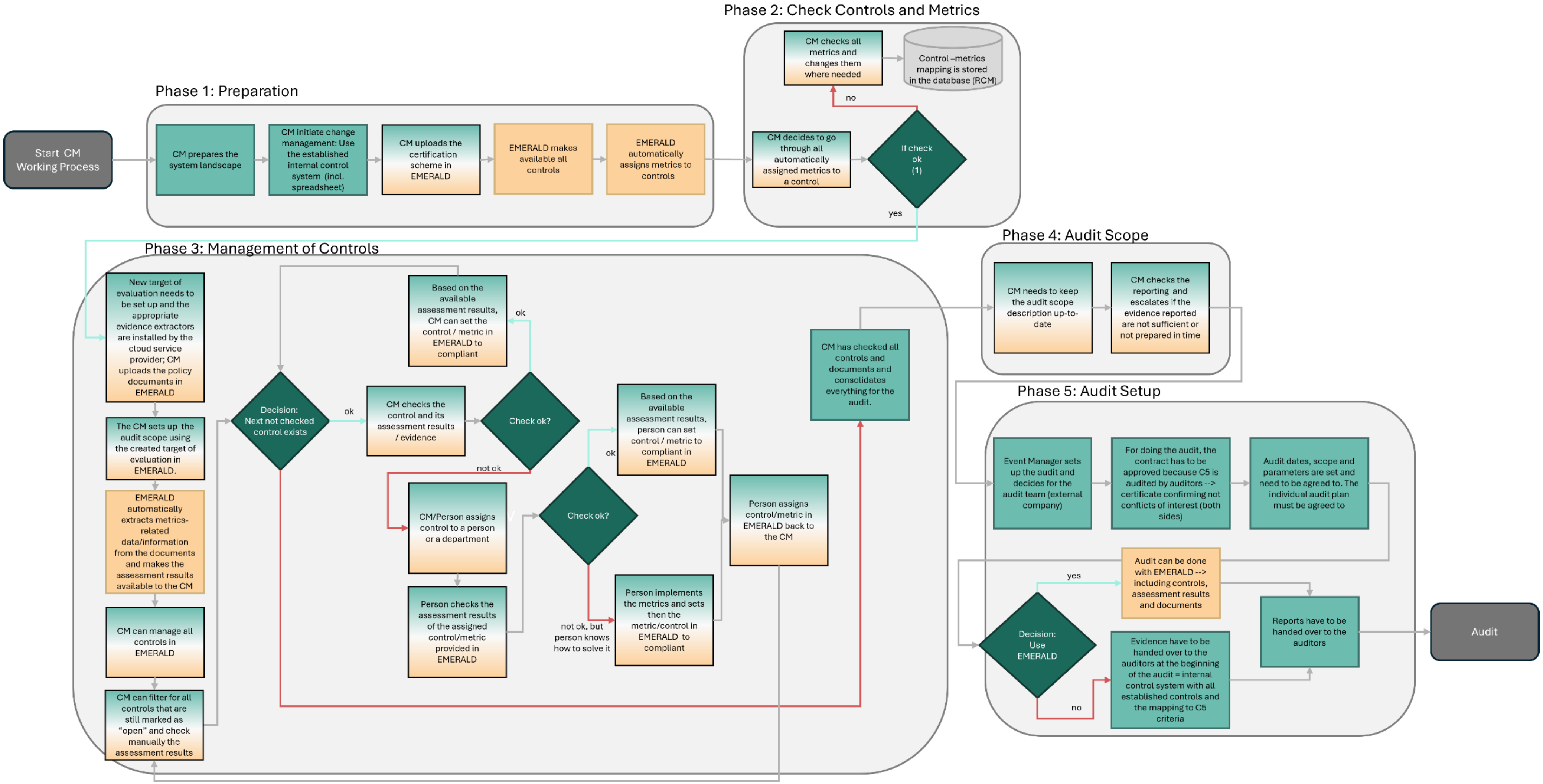

Start CM Working Process
Phase 1: Preparation
CM prepares the system landscape
CM initiate change management: Use the established internal control system (incl. spreadsheet)
CM uploads the certification scheme in EMERALD
EMERALD makes available all controls
EMERALD automatically assigns metrics to controls
Phase 2: Check Controls and Metrics
CM checks all metrics and changes them where needed
Control –metrics mapping is stored in the database (RCM)
no
CM decides to go through all automatically assigned metrics to a control
If check ok (1)
yes
Phase 3: Management of Controls
New target of evaluation needs to be set up and the appropriate evidence extractors are installed by the cloud service provider; CM uploads the policy documents in EMERALD
The CM sets up the audit scope using the created target of evaluation in EMERALD.
EMERALD automatically extracts metrics-related data/information from the documents and makes the assessment results available to the CM
CM can manage all controls in EMERALD
CM can filter for all controls that are still marked as "open" and check manually the assessment results
Decision: Next not checked control exists
ok
CM checks the control and its assessment results / evidence
Check ok?
ok
Based on the available assessment results, CM can set the control / metric in EMERALD to compliant
not ok
CM/Person assigns control to a person or a department
Person checks the assessment results of the assigned control/metric provided in EMERALD
Check ok?
ok
Based on the available assessment results, person can set control / metric to compliant in EMERALD
not ok, but person knows how to solve it
Person implements the metrics and sets then the metric/control in EMERALD to compliant
Person assigns control/metric in EMERALD back to the CM
CM has checked all controls and documents and consolidates everything for the audit.
Phase 4: Audit Scope
CM needs to keep the audit scope description up-to-date
CM checks the reporting and escalates if the evidence reported are not sufficient or not prepared in time
Phase 5: Audit Setup
Event Manager sets up the audit and decides for the audit team (external company)
For doing the audit, the contract has to be approved because C5 is audited by auditors --> certificate confirming not conflicts of interest (both sides)
Audit dates, scope and parameters are set and need to be agreed to. The individual audit plan must be agreed to
Audit can be done with EMERALD --> including controls, assessment results and documents
yes
Decision: Use EMERALD
no
Evidence have to be handed over to the auditors at the beginning of the audit = internal control system with all established controls and the mapping to C5 criteria
Reports have to be handed over to the auditors
Audit

Figure 5. IONOS – Workflow Representation with EMERALD support

4.2.2 Pilot 2: CloudFerro (CF)

We conducted two interviews with CloudFerro employees: one with a compliance manager and one with a security manager. Afterwards, we conducted a focus group with CloudFerro to validate our findings regarding the processes with them. From these discussions the simple process of how to prepare for an audit was derived. Figure 6 presents the simple process of an audit preparation process as it is now, while Figure 8 presents the simple process enhanced with the EMERALD support.

After having transferred the simple process into the workflow representation, we conducted a workshop with an employee from CloudFerro to discuss the workflow representation and to adapt it – if necessary. The CF workflow representation for the current audit preparation process without EMERALD support is presented in Figure 7, and the workflow representation with EMERALD support is presented in Figure 9.

In the following we present the simple process and the corresponding workflow presentation covering the audit preparation processes as they are now. Then we present the simple process and the elaborated workflow representation as they would look like using the EMERALD solution.

4.2.2.1 Simple Process without EMERALD support

The simple process without EMERALD support consists of the following four phases:

- **Phase 1 – Starting with analysis** (Figure 6, Phase 1): In phase 1, the responsible person starts with a coordination check and contacts the certification board. The audit preparation process differs a bit depending on whether the audit preparation is done for a new certification scheme, for an existing certification scheme that was updated, or for checking the current certification scheme. If a new certification scheme is added, more work is needed to fulfil all controls. If a certification scheme was updated, they check which controls were updated and which are new. Their goal is to implement as many controls as possible in the most efficient way.
- **Phase 2 – Standard** (Figure 6, Phase 2): In phase 2, the responsible person deals with the respective certification scheme to be prepared. They buy either the new standard or organize the updated standard. They go very carefully through the respective standard and elicit either all controls from the new standard or only the new and updated controls from the updated standard.
- **Phase 3 – Check with documentation** (Figure 6, Phase 3): All controls need to be clarified on how to deal with them if they need to be implemented (technically), if respective documents need to be updated, etc. Where necessary, other departments or individuals will be contacted to help clarify controls.
- **Phase 4 – Identify gaps** (Figure 6, Phase 4): In this phase, all existing gaps are identified to manage open controls and discuss how to deal with them.

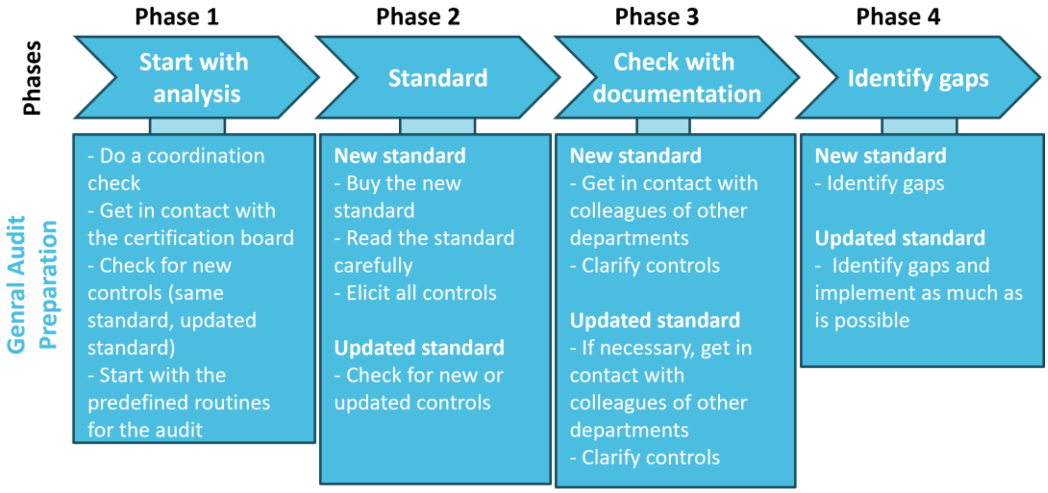

Phases
Phase 1
Start with analysis
Phase 2
Standard
Phase 3
Check with documentation
Phase 4
Identify gaps
Genral Audit Preparation
- Do a coordination check
- Get in contact with the certification board
- Check for new controls (same standard, updated standard)
- Start with the predefined routines for the audit
New standard
- Buy the new standard
- Read the standard carefully
- Elicit all controls
Updated standard
- Check for new or updated controls
New standard
- Get in contact with colleagues of other departments
- Clarify controls
Updated standard
- If necessary, get in contact with colleagues of other departments
- Clarify controls
New standard
- Identify gaps
Updated standard
- Identify gaps and implement as much as is possible

Figure 6. CloudFerro – Simple process representation without EMERALD support

4.2.2.2 Workflow Representation of the Process without EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from CloudFerro, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 7.

- **Phase 1 – Starting with analysis** (Figure 7, Phase 1):
  - Coordination check and standard: In the first phase, the CM does a coordination check and gets in contact with the certification board. Additionally, the CM checks the new or updated standard.
- **Phase 2 – Standard (Scheme)** (Figure 7, Phase 2):
  - Standard (scheme): Depending if the CM has to deal with the same standard as in the last audit, an updated version of the standard or a new standard, the CM needs to do different activities:
    - Same standard: No activities are required here.
    - Updated standard: CM needs to check for the new or updated controls in the standard.
    - New standard: CM needs to buy the new standard and get familiar with it. The CM has to extract all controls from the new standard.
- **Phase 3 – Check with documentation** (Figure 7, Phase 3):
  - Check documentation: The CM needs to check back the new or updated controls with the corresponding documents. The CM makes sure to find the exact information to fulfil the controls. The CM writes down their responses for each control and makes sure to provide the documentation and provide links to their solution.
  - Contact colleagues: As a CM does not always have all detailed domain knowledge about all controls, the CM contacts colleagues and/or departments to clarify the new or updated controls.
- **Phase 4 – Identify gaps** (Figure 7, Phase 4):
  - Identify gaps: The CM and their colleagues identify gaps in the documentation and try to implement as much for the new/updated control as possible.

- **Phase 5 – Managing controls** (Figure 7, Phase 5):
    - Spreadsheet or word document: Depending on the standard, the CM creates a spreadsheet or a word document in which all controls are managed. The CM creates new controls or updates existing controls and their progress of implementation.
    - Organizational and technical controls: For organizational controls, the CM checks if in some of their documents something is written about the control. Depending on the text found, the CM must decide: i) if the written text is ok, then nothing needs to be done; ii) if the written text needs to be updated in line with the control; or iii) if there is no written text referring to the control, then the text needs to be written. For the technical controls, the CM relies on best practices and the company's CI/CD to initiate the required implementation (software updates, implementation of security tools, configuration changes...).
    - Final check: Finally, the CM needs to consolidate everything for the audit. Afterwards the CM plans the audit with an external notified body and clarifies the details including the date, the audit scope, the target of evaluation, and other logistics.

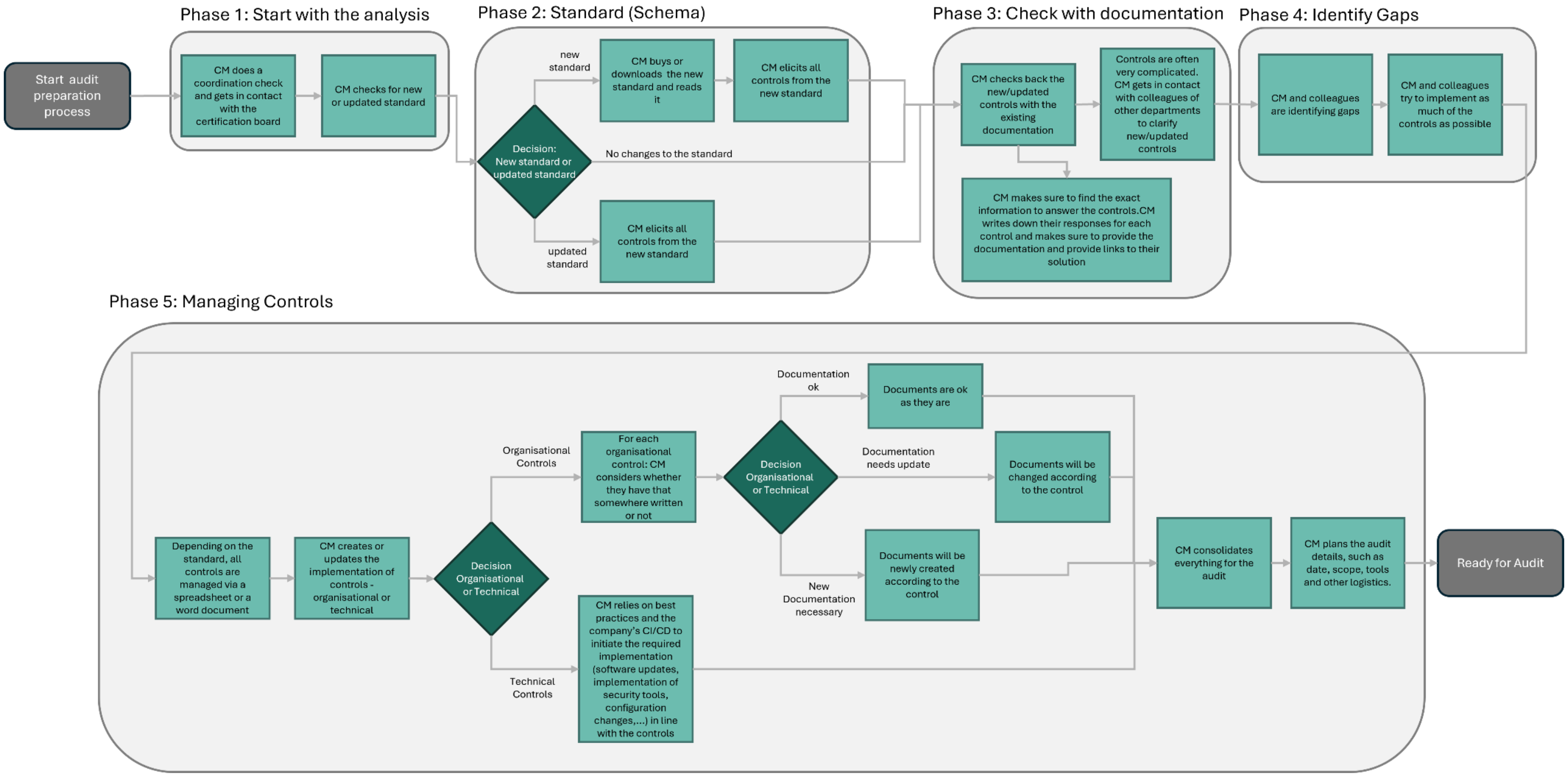

Phase 1: Start with the analysis
Phase 2: Standard (Schema)
Phase 3: Check with documentation
Phase 4: Identify Gaps
Start audit preparation process
CM does a coordination check and gets in contact with the certification board
CM checks for new or updated standard
new standard
CM buys or downloads the new standard and reads it
CM elicits all controls from the new standard
Decision: New standard or updated standard
No changes to the standard
updated standard
CM elicits all controls from the new standard
CM checks back the new/updated controls with the existing documentation
Controls are often very complicated. CM gets in contact with colleagues of other departments to clarify new/updated controls
CM makes sure to find the exact information to answer the controls.CM writes down their responses for each control and makes sure to provide the documentation and provide links to their solution
CM and colleagues are identifying gaps
CM and colleagues try to implement as much of the controls as possible
Phase 5: Managing Controls
Depending on the standard, all controls are managed via a spreadsheet or a word document
CM creates or updates the implementation of controls - organisational or technical
Decision Organisational or Technical
Organisational Controls
For each organisational control: CM considers whether they have that somewhere written or not
Technical Controls
CM relies on best practices and the company's CI/CD to initiate the required implementation (software updates, implementation of security tools, configuration changes,...) in line with the controls
Decision Organisational or Technical
Documentation ok
Documents are ok as they are
Documentation needs update
Documents will be changed according to the control
New Documentation necessary
Documents will be newly created according to the control
CM consolidates everything for the audit
CM plans the audit details, such as date, scope, tools and other logistics.
Ready for Audit

Figure 7. CloudFerro – Workflow Representation without EMERALD support

4.2.2.3 Simple Process with EMERALD support

For three of the four phases mentioned above in the CloudFerro audit preparation simple process (see Figure 6), we have derived some ideas on how the audit preparation process of cloud solutions at CloudFerro could be supported by the EMERALD UI, as shown in Figure 8.

- **Phase 1 – Initiation** (Figure 8, Phase 1): This phase is out of the scope of EMERALD.
- **Phase 2 – Standard** (Figure 8, Phase 2): EMERALD can support the CM with the following tasks for setting up a new standard or for dealing with an update of an existing standard:
    - New Standard**:** After having uploaded a new standard in EMERALD, the EMERALD UI can set-up the list of all controls extracted from the new standard. Additionally, it can provide the possibility to add the corresponding metrics for each control.
    - Update a Standard: EMERALD can support the upload of an updated standard.
- **Phase 3 – Check with documentation** (Figure 8, Phase 3): EMERALD can support the CM with the following tasks for setting up a new standard or for dealing with an update of an existing standard:
    - For a new standard as well as for an updated standard, EMERALD can help to derive evidence for organisational and technical controls.
- **Phase 4 – Identify gaps** (Figure 8, Phase4):
    - For a new standard as well as for an updated standard, EMERALD can show identified gaps and detected non-conformities for the new or the updated controls.

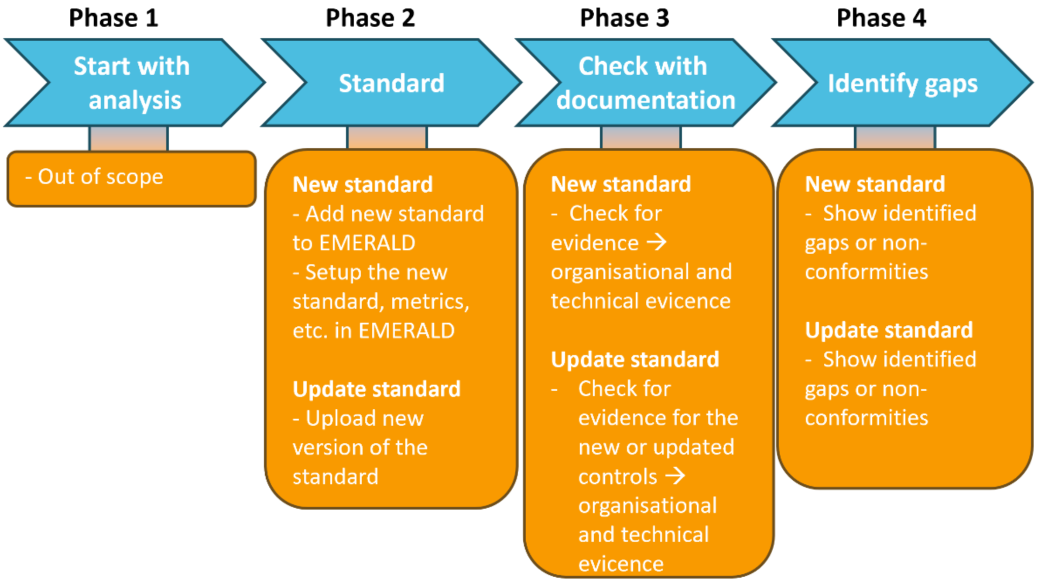

Phase 1
Start with analysis
- Out of scope
Phase 2
Standard
New standard
- Add new standard to EMERALD
- Setup the new standard, metrics, etc. in EMERALD
Update standard
- Upload new version of the standard
Phase 3
Check with documentation
New standard
- Check for evidence → organisational and technical evicence
Update standard
- Check for evidence for the new or updated controls → organisational and technical evicence
Phase 4
Identify gaps
New standard
- Show identified gaps or non-conformities
Update standard
- Show identified gaps or non-conformities

Figure 8. CloudFerro - Simple process representation with EMERALD support

4.2.2.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from CloudFerro, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 9.

- **Phase 1 – Start with the Analysis** (Figure 9, Phase 1): Starting the analysis for setting up an audit preparation process will still be managed by the CM outside of EMERALD:

  - Start with the analysis: The CM does a coordination check and gets in contact with the certification board to start the preparation of an audit. Then the CM gets the new or updated standard.
- **Phase 2 – Standard (Scheme)** (see Figure 9, Phase 2): EMERALD can support the CM with the following tasks:
  - Organize the new/updated standard/scheme: The CM looks for the new scheme – either the CM buys it or downloads it from a corresponding website.
  - Upload scheme: The CM brings the new/updated scheme in the corresponding format and can upload it into EMERALD. EMERALD makes all controls of the scheme available for the CM and automatically suggests metrics to the controls.
- **Phase 3-5: Managing Controls** (see Figure 9, Phase 3-5): EMERALD can support the CM with the following tasks:
  - Automatic assessment result extraction: EMERALD automatically extracts the assessment results for each metric of each control. EMERALD provides a view for the CM and presents a list of all controls and the respective assessment results for each audit scope.
  - Check controls: With the help of EMERALD, the CM can filter for all controls and metrics with respect to their states (compliant / non-compliant).
  - Deal with controls: The CM needs to check especially all non-compliant controls or open metrics. Depending on the assessment results and the domain knowledge of the CM, the CM can decide to set the control/metric to compliant (e.g., if only one assessment result is ok). Or the CM can also assign a control/metric to another person. The other person checks the control/metric and can decide to set the control/metric to compliant (e.g., if one of the provided assessment results is ok), or the person can also assign the control/metric to another person, who might know how to deal with the control/metric. Finally, all controls need to be assigned back to the CM.
  - Preparing for an audit: After the CM has checked all controls and all documents, the CM consolidates everything for the audit. In the next step the CM plans the audit with a notified body including date, scope, tools, logistics, etc.

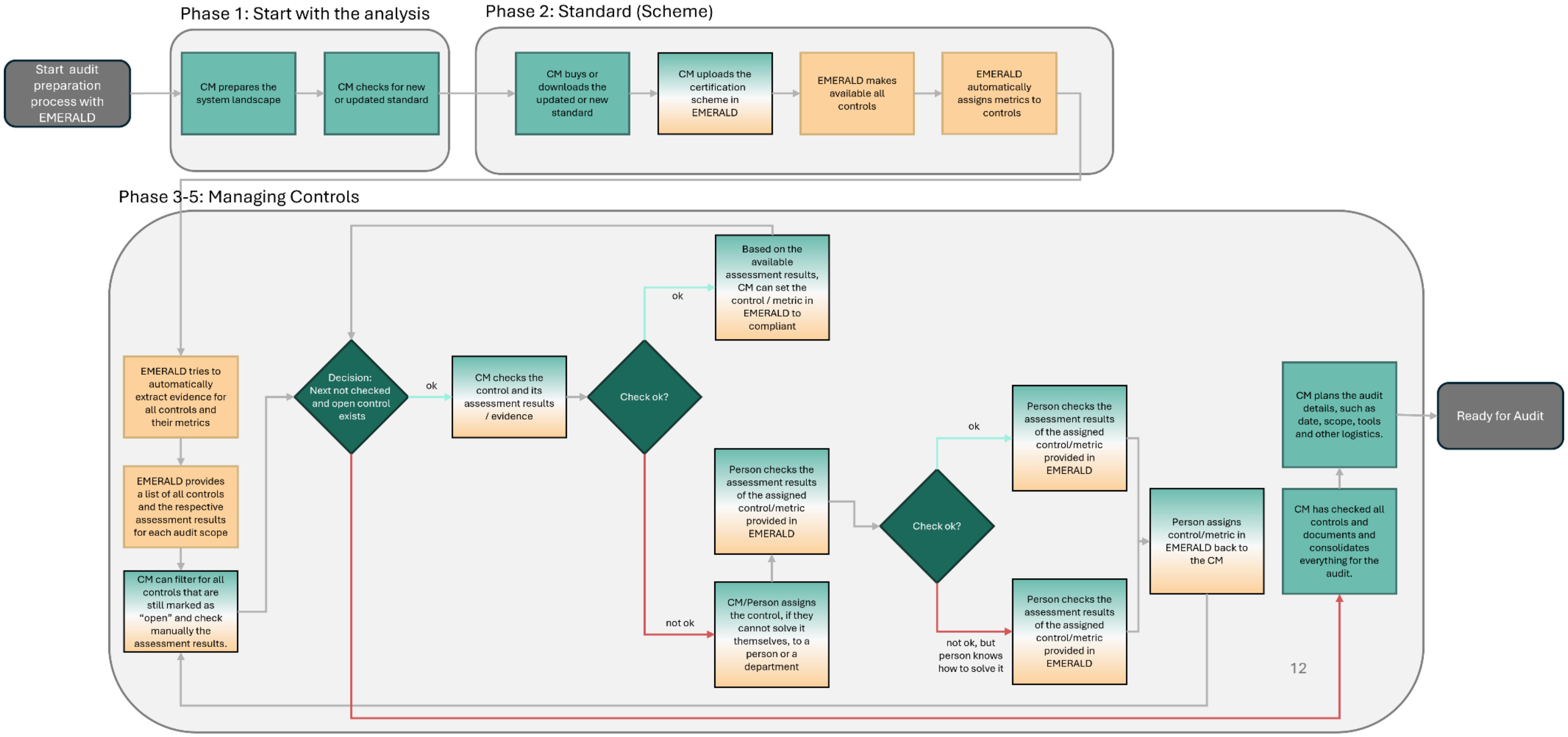

Phase 1: Start with the analysis
Phase 2: Standard (Scheme)
Start audit preparation process with EMERALD
CM prepares the system landscape
CM checks for new or updated standard
CM buys or downloads the updated or new standard
CM uploads the certification scheme in EMERALD
EMERALD makes available all controls
EMERALD automatically assigns metrics to controls
Phase 3-5: Managing Controls
EMERALD tries to automatically extract evidence for all controls and their metrics
EMERALD provides a list of all controls and the respective assessment results for each audit scope
CM can filter for all controls that are still marked as "open" and check manually the assessment results.
Decision: Next not checked and open control exists
ok
CM checks the control and its assessment results / evidence
Check ok?
ok
Based on the available assessment results, CM can set the control / metric in EMERALD to compliant
not ok
CM/Person assigns the control, if they cannot solve it themselves, to a person or a department
Person checks the assessment results of the assigned control/metric provided in EMERALD
Check ok?
ok
Person checks the assessment results of the assigned control/metric provided in EMERALD
not ok, but person knows how to solve it
Person checks the assessment results of the assigned control/metric provided in EMERALD
Person assigns control/metric in EMERALD back to the CM
CM has checked all controls and documents and consolidates everything for the audit.
CM plans the audit details, such as date, scope, tools and other logistics.
Ready for Audit
12

Figure 9. CloudFerro - Workflow Representation with EMERALD support

4.2.3 Pilot 3: Fabasoft (FABA)

We conducted an interview with three compliance managers from Fabasoft. Additionally, after having analysed the results, we conducted a focus group with the responsible compliance manager and the EMERALD project manager on behalf of FABA to get input and feedback about the derived simple processes. Figure 10 presents the simple process of an audit preparation process as it is now, while Figure 12 presents the simple process enhanced with the EMERALD support.

After having transformed the simple process representation into a workflow representation, we conducted two workshops with Fabasoft colleagues to validate the processes. Figure 11 presents the derived workflow representation of the simple process as it is now, and Figure 13 presents the workflow representation with EMERALD support.

First, we present the simple process and the corresponding workflow presentation covering the processes as they are now. Then we present the simple process and the elaborated workflow representation as it would look like using the EMERALD solution.

4.2.3.1 Simple Process without EMERALD support

The simple process without EMERALD support consists of the following three phases:

- **Phase 1 – Set-up Mapping** (see Figure 10, Phase 1): In phase 1 of setting up the audit preparation for a new standard, all controls are added into a spreadsheet. This means that each control is presented in an individual line. For each of the controls, a set of parameters will be created and collected in phase 2.
- **Phase 2 – Mapping** (see Figure 10, Phase 2): In this phase, the compliance manager starts filling in the spreadsheet for all controls as far as possible. Controls that the compliance manager cannot fill in are assigned to other departments or individual persons, who are responsible that the respective controls are fulfilled.
- **Phase 3 – Verification** (see Figure 10, Phase 3): In the verification phase, the compliance manager must check whether all controls have been filled-in in the spreadsheet and whether all controls have been assigned correct and concrete evidence that can be shown to the auditors.

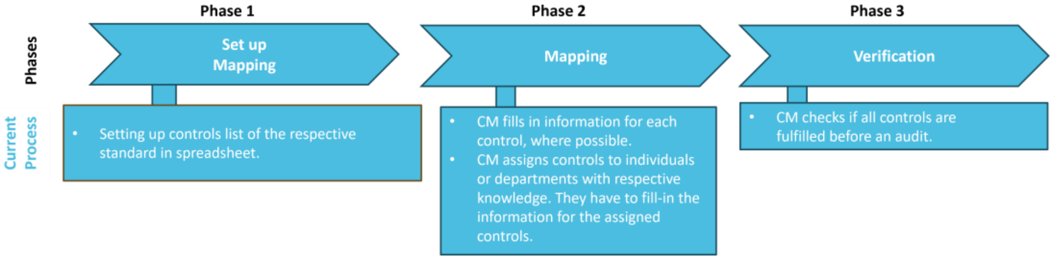

Phases
Current Process
Phase 1
Set up Mapping
Setting up controls list of the respective standard in spreadsheet.
Phase 2
Mapping
CM fills in information for each control, where possible.
CM assigns controls to individuals or departments with respective knowledge. They have to fill-in the information for the assigned controls.
Phase 3
Verification
CM checks if all controls are fulfilled before an audit.

Figure 10. Fabasoft – Simple process representation without EMERALD support

4.2.3.2 Workflow Representation of the Process without EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from Fabasoft, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 11.

- **Phase 1 – Set-up Mapping** (see Figure 11, Phase 1): In phase 1 of setting up the audit preparation for a new standard, the CM opens the certification scheme and copies all controls of the scheme into a spreadsheet.
- **Phase 2 – Mapping** (see Figure 11, Phase 2): In this phase, the CM starts filling in the spreadsheet for all controls as far as possible. The CM goes through all controls. Where possible, the CM adds the respective evidence to a control. If the CM needs some input from a colleague or a department, the CM assigns the control to the respective person or department. The assigned person can either add the respective evidence to the control or assigns the control back to the CM. If the assigned person cannot provide the respective evidence, the person can either assign the control to another person or back to the CM.
- **Phase 3 – Verification** (see Figure 11, Phase 3): After all controls and the respective evidence have been dealt, the CM must check in the verification phase whether all controls have been filled-in in the spreadsheet and whether all controls have attached concrete evidence that can be shown to the auditors.

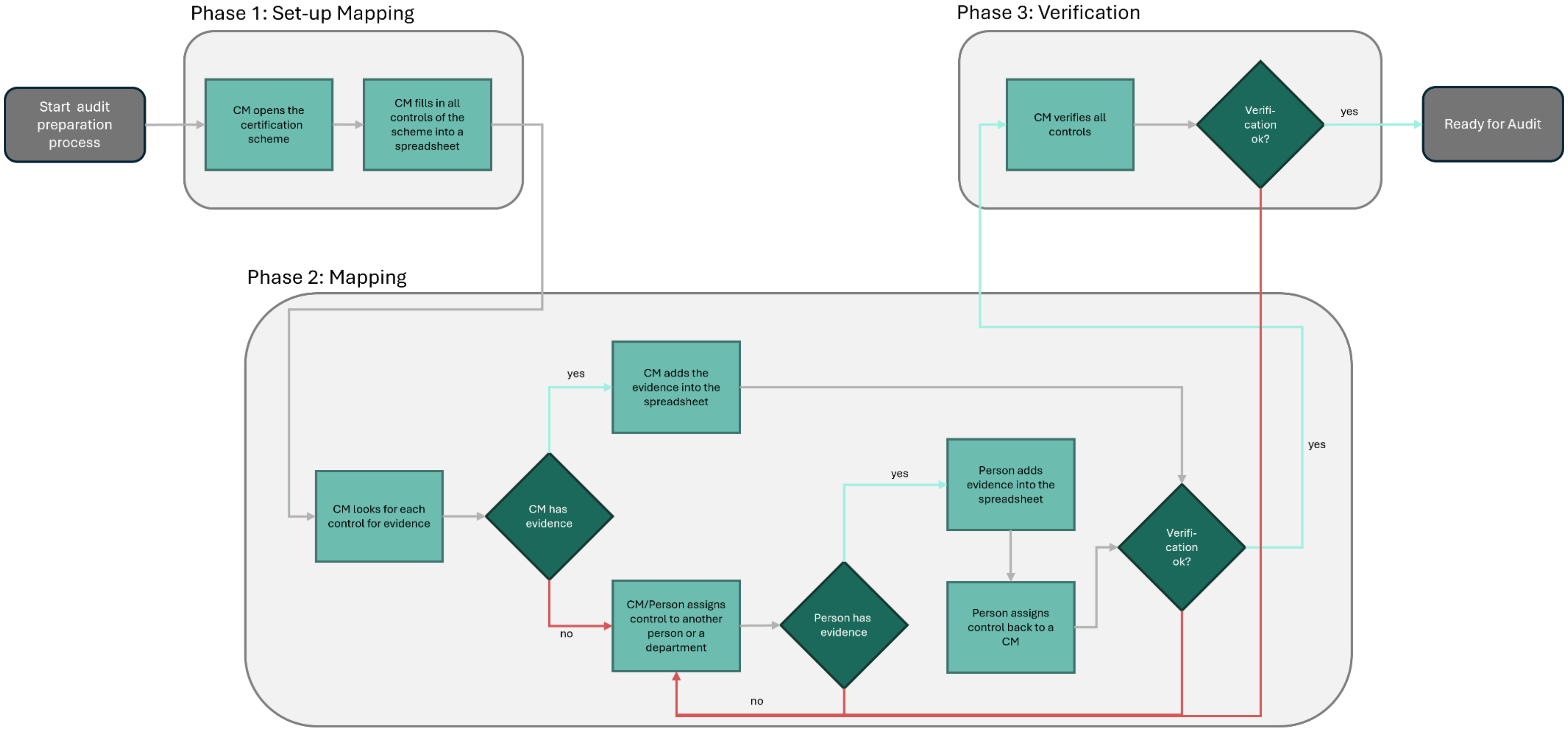
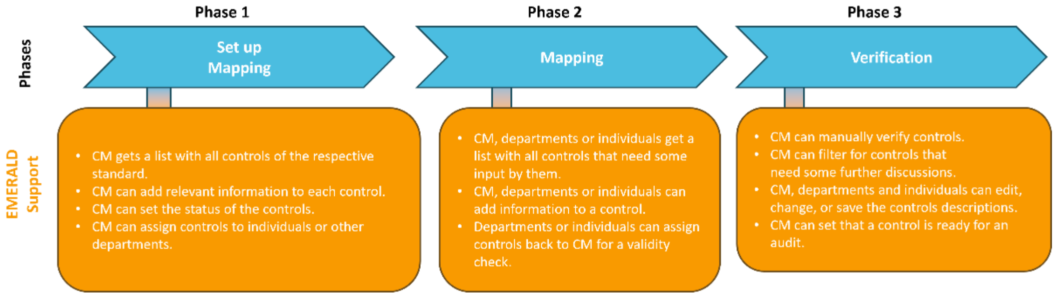

Phase 1: Set-up Mapping
Phase 3: Verification
Phase 2: Mapping
Start audit preparation process
CM opens the certification scheme
CM fills in all controls of the scheme into a spreadsheet
CM verifies all controls
Verifi-cation ok?
yes
Ready for Audit
yes
CM adds the evidence into the spreadsheet
CM looks for each control for evidence
CM has evidence
no
CM/Person assigns control to another person or a department
Person has evidence
no
yes
Person adds evidence into the spreadsheet
Person assigns control back to a CM
Verifi-cation ok?
yes

Figure 11. Fabasoft – Workflow Representation without EMERALD support

4.2.3.3 Simple Process with EMERALD support

For each of the three phases mentioned above in the Fabasoft audit preparation process, we have derived some ideas on how the audit preparation process of cloud solutions at Fabasoft could be supported by the EMERALD UI, as shown in Figure 12.

- **Phase 1 – Set-up Mapping** (Figure 12, Phase 1): EMERALD can support the compliance manager with the following tasks for setting up the mapping:
  - Control overview: EMERALD can create a list with all controls of the respective certification scheme for the upcoming audit.
  - Control metrics: EMERALD can provide the possibility to set the respective metrics for all controls.
  - Control status: EMERALD can show the status of each control on two levels – compliance level and status level.
- **Phase 2 – Set-up** (Figure 12, Phase 2): EMERALD can support the compliance manager with the following tasks:
  - Filtering: EMERALD allows to filter for controls that need further input.
  - Add notes: EMERALD allows to add notes to a control e.g., suggestions on how a control could be addressed.
  - Assigning controls: EMERALD allows to assign controls to departments or individuals and vice versa, controls can be assigned back to the compliance manager.
- **Phase 3 – Verification** (Figure 12, Phase 3): EMERALD can support the compliance manager and the other departments with the following tasks during the verification phase:
  - Verification by departments or individuals: EMERALD allows the respective departments or individuals to verify the controls.
  - Verification by the compliance managers: EMERALD allows the compliance manager to mark the respective controls as ready for being used in an audit.



- CM gets a list with all controls of the respective standard.
- CM can add relevant information to each control.
- CM can set the status of the controls.
- CM can assign controls to individuals or other departments.

- CM, departments or individuals get a list with all controls that need some input by them.
- CM, departments or individuals can add information to a control.
- Departments or individuals can assign controls back to CM for a validity check.

- CM can manually verify controls.
- CM can filter for controls that need some further discussions.
- CM, departments and individuals can edit, change, or save the controls descriptions.
- CM can set that a control is ready for an audit.

Figure 12. Fabasoft – Simple process representation with EMERALD support

4.2.3.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from Fabasoft, to investigate, if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 13.

- **Phase 1 – Set-up Mapping** (Figure 13, Phase 1): EMERALD can support the compliance manager with the following tasks for setting up the mapping:
  - Setup the certification scheme: Using EMERALD, the CM can either upload a new certification scheme or use an existing scheme that is available in EMERALD. EMERALD makes the scheme and all respective controls available and automatically assigns metrics to the controls.

  - Check metrics: The CM uses EMERALD to check all suggested metrics that were assigned to a control and can decide if the metrics are ok or need to be changed.
  - Setup target of evaluation: After having set up the scheme and assigned for each control the respective metrics, the CM sets up a target of evaluation. Additionally, the CM can (with the help of the IT department) set up the respective evidence extractors (e.g., *AI-SEC*, *AMOE*, *Clouditor Discovery*, *Codyze*, *eknows-e3*).
  - Setup Audit Scope: Finally, the CM creates a new audit scope in EMERALD using the newly created target of evaluation and the respective certification scheme, including its controls and metrics.
- **Phase 2 – Mapping** (Figure 13, Phase 1): In the mapping phase, EMERALD can support the compliance manager with the following tasks:
  - Automatic evidence extraction: EMERALD tries to automatically extract evidence for all controls and their metrics. The EMERALD UI presents a list of all controls and metrics and the extracted assessment results from the evidence extractors.
  - Filter controls: The CM can filter for all controls and metrics and check manually all assessment results.
  - CM checks non-compliant controls/open metrics: Especially for those controls or metrics that are non-compliant or open the CM needs to decide what to do. First, the CM checks the assessment results. Depending on the assessment results and depending on the CMs domain knowledge, the CM has two options: i) the CM can decide for a control that the assessment results (or at least one assessment results) for metric(s) are ok and change the metric status to ok; ii) the CM can assign the control or metric to another person or department.
  - Person checks non-compliant controls/open metrics: If a CM assigns a control or metric to an individual, that person must review the corresponding assessment results. This person has three possible courses of action:
    - If the person possesses the necessary domain knowledge, they verify the accuracy of at least one of the provided assessment results, mark the control as compliant or the metric as done, and return it to the CM.
    - If the person can implement the metric's measurement, the person proceeds with the implementation, documents the actions taken, and then reassigns the control or metric to the CM.
    - If the person lacks the expertise to implement the control or metric, the person either returns it to the CM or forwards it to another individual who might have the required knowledge. Ultimately, all controls should be reassigned to the CM.
- **Phase 3 – Verification** (Figure 13, Phase 3): EMERALD can support the compliance manager and the other departments with the following tasks during the verification phase:
  - Validity check: In the final phase of the process, the CM does a validity check, thus, a final check that all respective controls are compliant.
  - Filter for controls: To do so the CM goes through all controls again, checks all controls especially those that have been assigned back to the CM or need more discussions.

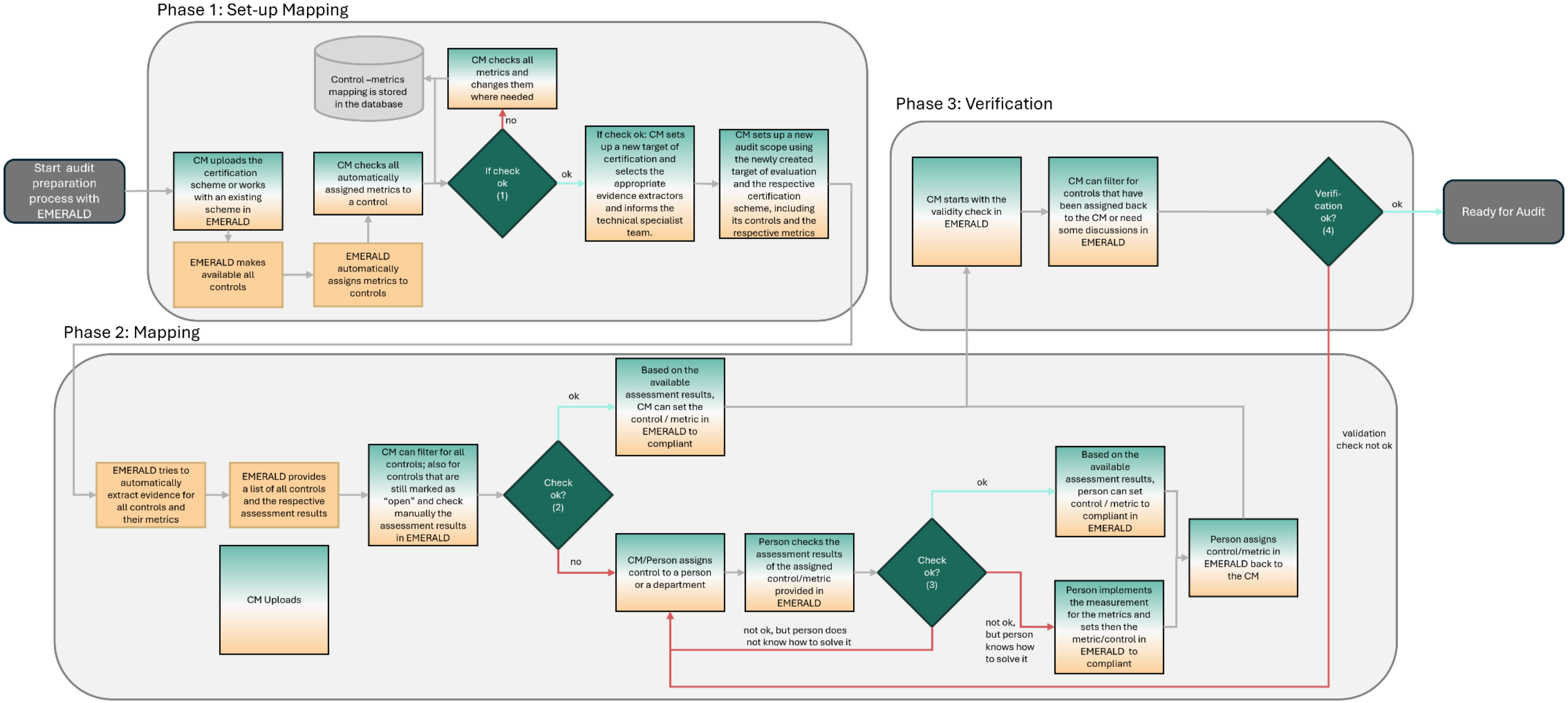

Phase 1: Set-up Mapping
Start audit preparation process with EMERALD
CM uploads the certification scheme or works with an existing scheme in EMERALD
EMERALD makes available all controls
EMERALD automatically assigns metrics to controls
CM checks all automatically assigned metrics to a control
Control –metrics mapping is stored in the database
CM checks all metrics and changes them where needed
no
If check ok (1)
ok
If check ok: CM sets up a new target of certification and selects the appropriate evidence extractors and informs the technical specialist team.
CM sets up a new audit scope using the newly created target of evaluation and the respective certification scheme, including its controls and the respective metrics
Phase 3: Verification
CM starts with the validity check in EMERALD
CM can filter for controls that have been assigned back to the CM or need some discussions in EMERALD
Verifi-cation ok? (4)
ok
Ready for Audit
validation check not ok
Phase 2: Mapping
EMERALD tries to automatically extract evidence for all controls and their metrics
EMERALD provides a list of all controls and the respective assessment results
CM can filter for all controls; also for controls that are still marked as "open" and check manually the assessment results in EMERALD
CM Uploads
Check ok? (2)
ok
no
Based on the available assessment results, CM can set the control / metric in EMERALD to compliant
CM/Person assigns control to a person or a department
Person checks the assessment results of the assigned control/metric provided in EMERALD
Check ok? (3)
ok
not ok, but person does not know how to solve it
not ok, but person knows how to solve it
Based on the available assessment results, person can set control / metric to compliant in EMERALD
Person implements the measurement for the metrics and sets then the metric/control in EMERALD to compliant
Person assigns control/metric in EMERALD back to the CM

Figure 13. Fabasoft - Workflow Representation with EMERALD support

4.2.4 Pilot 4: CaixaBank (CXB)

With CXB, we conducted a written interview with compliance managers. Additionally, after having analysed the results, we conducted a focus group with the responsible compliance manager and the project manager on behalf of CXB for EMERALD to get input and feedback about the derived simple processes. Figure 14 presents the current simple process of an audit preparation process referring to a cloud service provider where CXB is a customer, while Figure 16 presents the simple process enhanced with the EMERALD support.

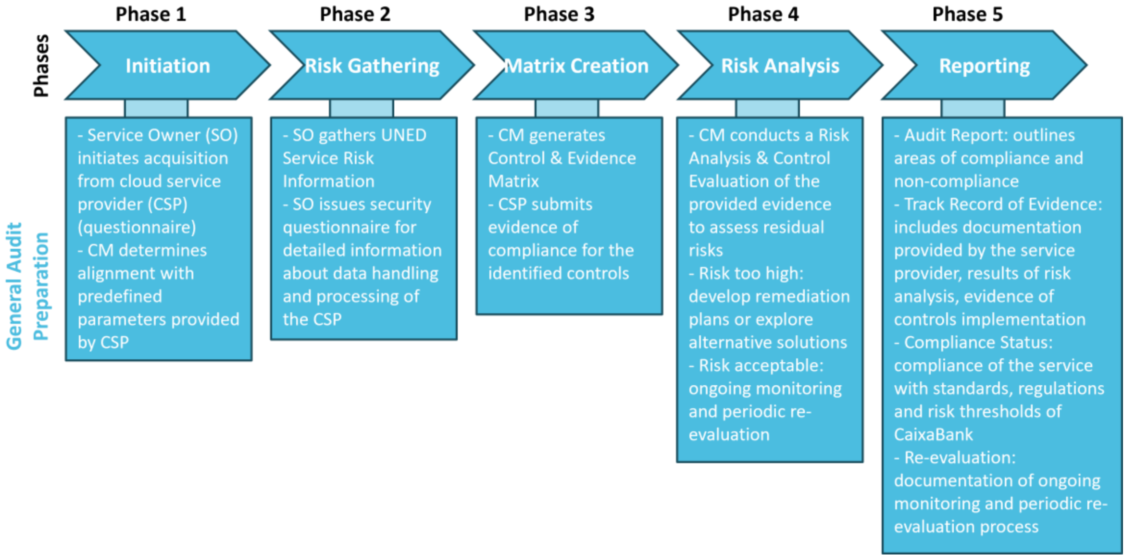
After having transformed the simple process representation into a workflow representation, we conducted a workshop with the CXB colleagues to validate the processes. Figure 15 presents the derived workflow representation of the simple process as it is now, and Figure 17 presents the workflow representation with EMERALD support.

First, we present the simple process and the corresponding workflow presentation covering the processes as they are now. Then, we present the simple process and the elaborated workflow representation as it would look like using the EMERALD solution.

4.2.4.1 Simple Process without EMERALD support

The simple process without EMERALD support consists of the following five phases:

- **Phase 1 – Initiation** (Figure 14, Phase 1): The service owner (SO) of CXB initiates the information acquisition from a cloud service provider (CSP) with the help of the questionnaire. When having received the filled in questionnaire from the CSP, the CM determines alignment with predefined parameters provided by the CSP.
- **Phase 2 – Risk Gathering** (Figure 14, Phase 2): The service provider (SP) gathers the UNED Service Risk Information. Based on this information, the SO issues the security questionnaire to the CSP to collect detailed information about their data handling and data processing.
- **Phase 3 – Matrix Creation** (Figure 14, Phase 3): With the help of the information collected from the second questionnaire, the CM generates the control & evidence matrix for managing the CSPs controls. Then the CM asks the CSP to submit the evidence of compliance for the identified controls to CXB.
- **Phase 4 – Risk Analysis** (Figure 14, Phase 4): Based on the evidence received, the CM conducts a risk analysis and control evaluation to assess residual risks. If the risk of an evidence for a control is too high, the CM develops remediation plans or explore alternative solutions. If the risk of evidence is acceptable, the CM performs a continuous monitoring and periodic re-evaluation of the controls, and the evidence assigned.
- **Phase 5 – Reporting** (Figure 14, Phase 5): In this phase different reports are created:
  - Audit Report: outlines areas of compliance and non-compliance.
  - Track Record of Evidence: includes documentation provided by the CSP, results of risk analysis, evidence of the implementation of controls.
  - Compliance Status: documents the compliance of the service with standards, regulations and risk thresholds of CaixaBank.
  - Re-evaluation: provides the documentation of ongoing monitoring and periodic re-evaluation process.



- Service Owner (SO) initiates acquisition from cloud service provider (CSP) (questionnaire)
- CM determines alignment with predefined parameters provided by CSP

- SO gathers UNED Service Risk Information
- SO issues security questionnaire for detailed information about data handling and processing of the CSP

- CM generates Control & Evidence Matrix
- CSP submits evidence of compliance for the identified controls

- CM conducts a Risk Analysis & Control Evaluation of the provided evidence to assess residual risks
- Risk too high: develop remediation plans or explore alternative solutions
- Risk acceptable: ongoing monitoring and periodic re-evaluation

- Audit Report: outlines areas of compliance and non-compliance
- Track Record of Evidence: includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation
- Compliance Status: compliance of the service with standards, regulations and risk thresholds of CaixaBank
- Re-evaluation: documentation of ongoing monitoring and periodic re-evaluation process

Figure 14. CaixaBank – Simple process representation without EMERALD support

4.2.4.2 Workflow Representation of the Process without EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from CXB, to investigate if the workflow representation is correct. After some improvements, the resulting workflow process is presented in Figure 15.

- **Phase 1 – Initiation** (Figure 15, Phase 1):
  - Initiating the process: The Service Owner is initiating the acquisition of information from a third-party cloud service provider by sending out a questionnaire.
  - Governance and compliance review: When having received the filled in questionnaire from the CSP, the CM reviews the governance and compliance information to determine its alignment with predefined parameters, considering data types and processing locations provided by the CSP.
- **Phase 2 – Risk Gathering** (Figure 15, Phase 2):
  - Risk gathering: The CSP needs to gather the service risk information focusing on various risk taxonomies like legal, business continuity, IT, and security.
  - Security questionnaire: The SO issues the security questionnaire to the CSP to gather detailed information about their data handling practices, including the types of information processed, data processing locations, and handling methods. This questionnaire is designed to assess the provider’s compliance with specific security controls.
- **Phase 3 – Matrix Creation** (Figure 15, Phase 3):
  - Control-evidence matrix: The CM generates a control and evidence matrix based on the service type and the information provided in the security questionnaire. The control matrix, which is predefined, is then sent to the CSP.
  - The CSP provides evidence of compliance for the identified controls, such as security certifications and policies.
- **Phase 4 – Risk Analysis** (Figure 15, Phase 4):
  - Based on the evidence received, the CM conducts a risk analysis and control evaluation to assess residual risks against the acceptable threshold. Depending on the risk assessment, the following options are possible (two options for risks above the threshold):

        - Risks too high (above threshold): The CSP needs to develop remediation plans and explore alternative solutions.
        - Risks too high (above threshold): The CSP needs to send other solutions or means to mitigate the risk.
        - Risk acceptable: The CM continues the monitoring and periodic re-evaluation of the controls and their evidence to ensure continued compliance and address any changes as needed.

- **Phase 5 – Reporting** (Figure 15, Phase 5): In this phase the different types of reports are created:
    - Audit Report: This document compiled by auditors summarizes the findings of the audit process. It outlines areas of compliance and identifies any non-compliance issues.
    - Track Record of Evidence: A comprehensive record of evidence is gathered and maintained. This evidence includes documentation provided by the service provider, results of risk analysis, evidence of controls.
    - Compliance Status: The audit process results in a determination of the compliance status of the service in question. It indicates whether the service meets the established standards, regulations, and risk threshold.
    - Categorization of the Service: The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly.

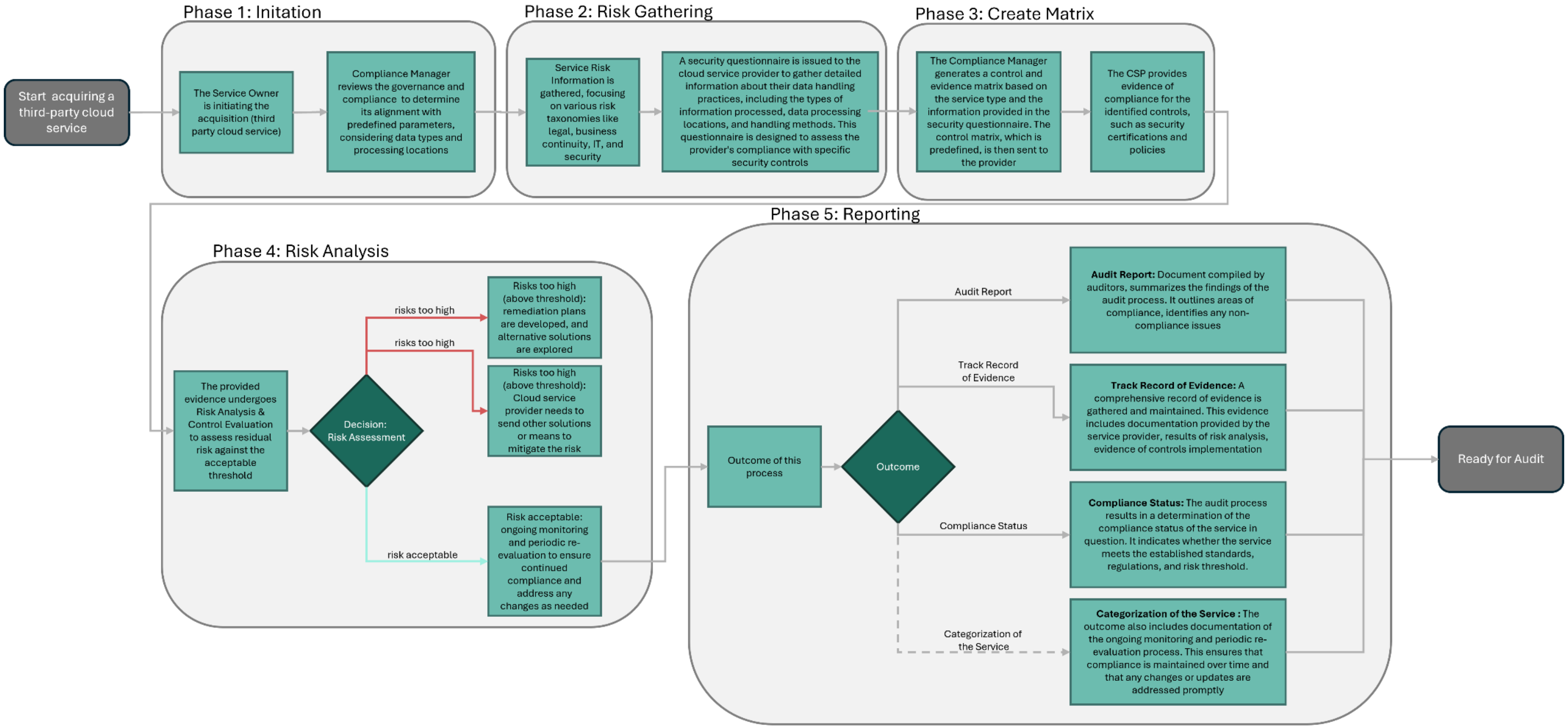

Start acquiring a third-party cloud service
Phase 1: Initation
The Service Owner is initiating the acquisition (third party cloud service)
Compliance Manager reviews the governance and compliance to determine its alignment with predefined parameters, considering data types and processing locations
Phase 2: Risk Gathering
Service Risk Information is gathered, focusing on various risk taxonomies like legal, business continuity, IT, and security
A security questionnaire is issued to the cloud service provider to gather detailed information about their data handling practices, including the types of information processed, data processing locations, and handling methods. This questionnaire is designed to assess the provider's compliance with specific security controls
Phase 3: Create Matrix
The Compliance Manager generates a control and evidence matrix based on the service type and the information provided in the security questionnaire. The control matrix, which is predefined, is then sent to the provider
The CSP provides evidence of compliance for the identified controls, such as security certifications and policies
Phase 4: Risk Analysis
The provided evidence undergoes Risk Analysis & Control Evaluation to assess residual risk against the acceptable threshold
Decision: Risk Assessment
risks too high
Risks too high (above threshold): remediation plans are developed, and alternative solutions are explored
risks too high
Risks too high (above threshold): Cloud service provider needs to send other solutions or means to mitigate the risk
risk acceptable
Risk acceptable: ongoing monitoring and periodic re-evaluation to ensure continued compliance and address any changes as needed
Phase 5: Reporting
Outcome of this process
Outcome
Audit Report
Audit Report: Document compiled by auditors, summarizes the findings of the audit process. It outlines areas of compliance, identifies any non-compliance issues
Track Record of Evidence
Track Record of Evidence: A comprehensive record of evidence is gathered and maintained. This evidence includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation
Compliance Status
Compliance Status: The audit process results in a determination of the compliance status of the service in question. It indicates whether the service meets the established standards, regulations, and risk threshold.
Categorization of the Service
Categorization of the Service : The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly
Ready for Audit

Figure 15. CaixaBank – Workflow Representation without EMERALD support

4.2.4.3 Simple Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from CXB, to investigate, if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 16.

- **Phase 1 – Initiation** (Figure 16, Phase 1): This phase is out of the scope of EMERALD.
- **Phase 2 – Risk Gathering** (Figure 16, Phase 2): This phase is out of the scope of EMERALD.
- **Phase 3 – Matrix Creation** (Figure 16, Phase 3): EMERALD can provide support by creating the controls and evidence matrix. Additionally, EMERALD can provide support by providing a possibility for managing customized security schemes.
- **Phase 4 – Risk Analysis** (Figure 16, Phase 4): The CSP can use EMERALD to provide evidence for the controls to the CM of CXB. The CM can then use EMERALD as a baseline to do the risk analysis.
- **Phase 5 – Reporting** (Figure 16, Phase 5): The EMERALD UI could help with the creation of some reports such as the outcome of an audit (overview of controls and evidence), tracking the record of evidence, compliance state of controls and evidence and re-evaluation.

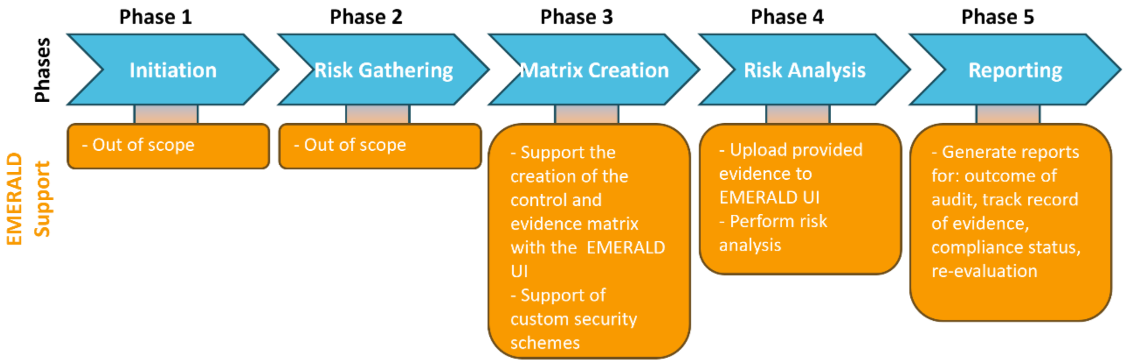

Phases
Phase 1
Initiation
Phase 2
Risk Gathering
Phase 3
Matrix Creation
Phase 4
Risk Analysis
Phase 5
Reporting
EMERALD Support
- Out of scope
- Out of scope
- Support the creation of the control and evidence matrix with the EMERALD UI
- Support of custom security schemes
- Upload provided evidence to EMERALD UI
- Perform risk analysis
- Generate reports for: outcome of audit, track record of evidence, compliance status, re-evaluation

Figure 16. CaixaBank – Simple process representation with EMERALD support

4.2.4.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from CXB, to investigate, if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 17.

- **Phase 1 – Initiation** (Figure 17, Phase 1): This phase is out of the scope of EMERALD.
  - Initiating the Process: The Service Owner initiates the acquisition of information from a third-party cloud service provider by sending out a questionnaire.
  - When having received the filled-in questionnaire from the CSP, the CM reviews the governance and compliance information to determine its alignment with predefined parameters, considering data types and processing locations provided by the CSP.
- **Phase 2 – Risk Gathering** (Figure 17, Phase 2): This phase is out of the scope of EMERALD.
  - Risk Gathering: The service provider (SP) needs to gather the service risk information focusing on various risk taxonomies like legal, business continuity, IT, and security.
  - Security Questionnaire: The SO issues the security questionnaire to the cloud service provider to gather detailed information about their data handling practices,

including the types of information processed, data processing locations, and handling methods. This questionnaire is designed to assess the providers' compliance with specific security controls.

- **Phase 3 – Matrix Creation** (Figure 17, Phase 3):
  - Define Own Certification Scheme: In EMERALD, CXB can define their own certification scheme based on the answers provided by the questionnaire from the CSPs – using existing controls from different schemes and defining their own controls.
  - Replace Control and Evidence Matrix: By setting up an audit scope with a target of evaluation and with the new certification scheme, EMERALD can replace the CXB control and evidence matrix.
  - Provide Access to EMERALD: The service owner provides the CSP access to EMERALD instance, and they set up the EMERALD evidence extractors.
  - Automatic Evidence Extraction: EMERALD tries to extract evidence for all controls and their metrics automatically.
  - List of Controls and Assessment Results: EMERALD provides a list of all controls and their respective assessment results and the CSP can ensure that everything is set up.
  - CSP informs CXB: CSP informs the service owner that everything is set up and the service owner informs the compliance manager.
- **Phase 4 – Risk Analysis** (Figure 17, Phase 4):
  - Check Controls and Assessment Results: CM checks the controls and their assessment results / evidence in EMERALD.
  - Risk Analysis & Control Evaluation: The evidence provided undergoes a risk analysis & control evaluation to assess residual risk against the acceptable threshold. Depending on the risk assessment, the following options exist (two options for risks above the threshold):
    - Risks too high (above threshold): The CSP needs to develop remediation plans and explore alternative solutions.
    - Risks too high (above threshold): The CSP needs to send other solutions or means to mitigate the risk.
    - Risk acceptable: The CM continues the monitoring and periodic re-evaluation of the controls and their evidence to ensure continued compliance and addresses any changes as needed.
- **Phase 5 – Reporting** (Figure 17, Phase 5): In this phase different types of reports are created, where EMERALD might support the report creation:
  - Audit Report: This document compiled by auditors summarizes the findings of the audit process. It outlines areas of compliance and identifies any non-compliance issues.
  - Track Record of Evidence: A comprehensive record of evidence is gathered and maintained. This evidence includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation.
  - Compliance Status: The audit process results in a determination of the compliance status of the service in question. The compliance status indicates whether the service meets the established standards, regulations, and risk threshold.
  - Categorization of the Service: The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly.

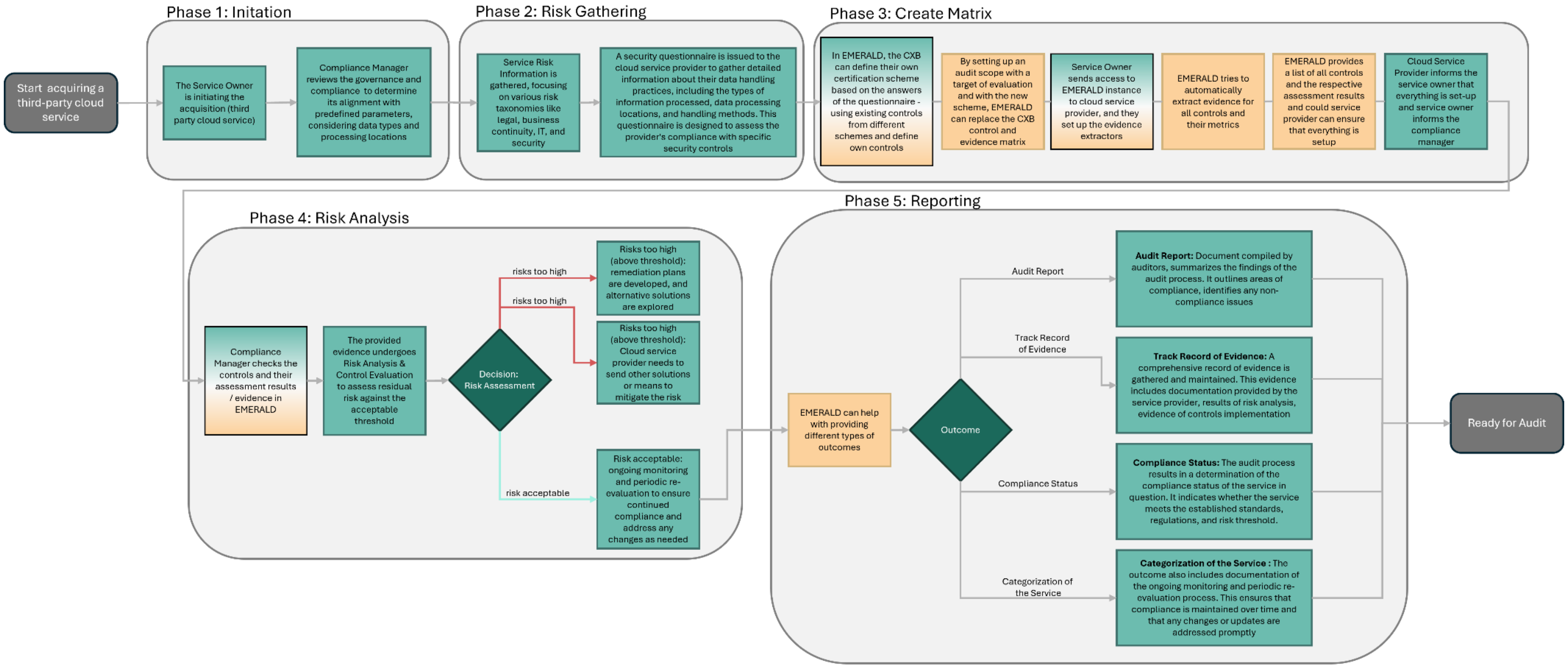

Start acquiring a third-party cloud service
Phase 1: Initation
The Service Owner is initiating the acquisition (third party cloud service)
Compliance Manager reviews the governance and compliance to determine its alignment with predefined parameters, considering data types and processing locations
Phase 2: Risk Gathering
Service Risk Information is gathered, focusing on various risk taxonomies like legal, business continuity, IT, and security
A security questionnaire is issued to the cloud service provider to gather detailed information about their data handling practices, including the types of information processed, data processing locations, and handling methods. This questionnaire is designed to assess the provider's compliance with specific security controls
Phase 3: Create Matrix
In EMERALD, the CXB can define their own certification scheme based on the answers of the questionnaire - using existing controls from different schemes and define own controls
By setting up an audit scope with a target of evaluation and with the new scheme, EMERALD can replace the CXB control and evidence matrix
Service Owner sends access to EMERALD instance to cloud service provider, and they set up the evidence extractors
EMERALD tries to automatically extract evidence for all controls and their metrics
EMERALD provides a list of all controls and the respective assessment results and could service provider can ensure that everything is setup
Cloud Service Provider informs the service owner that everything is set-up and service owner informs the compliance manager
Phase 4: Risk Analysis
Compliance Manager checks the controls and their assessment results / evidence in EMERALD
The provided evidence undergoes Risk Analysis & Control Evaluation to assess residual risk against the acceptable threshold
Decision: Risk Assessment
risks too high
risks too high
Risks too high (above threshold): remediation plans are developed, and alternative solutions are explored
Risks too high (above threshold): Cloud service provider needs to send other solutions or means to mitigate the risk
risk acceptable
Risk acceptable: ongoing monitoring and periodic re-evaluation to ensure continued compliance and address any changes as needed
Phase 5: Reporting
EMERALD can help with providing different types of outcomes
Outcome
Audit Report
Track Record of Evidence
Compliance Status
Categorization of the Service
Audit Report: Document compiled by auditors, summarizes the findings of the audit process. It outlines areas of compliance, identifies any non-compliance issues
Track Record of Evidence: A comprehensive record of evidence is gathered and maintained. This evidence includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation
Compliance Status: The audit process results in a determination of the compliance status of the service in question. It indicates whether the service meets the established standards, regulations, and risk threshold.
Categorization of the Service : The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly
Ready for Audit

Figure 17. CaixaBank – Workflow Representation with EMERALD support

4.2.5 Auditors (NIXU/DNV)

We conducted an interview with three auditors from NIXU/DNV. Additionally, after having analysed the results, we conducted a focus group with the responsible auditors and the NIXU/DNV EMERALD project manager to get input and feedback about the derived simple processes. Figure 18 presents the simple process of an audit preparation process as it is now, while Figure 20 presents the simple process enhanced with the EMERALD support.

After having transformed the simple process representation into a workshop representation without and with EMERALD support, we have conducted two workshops with NIXU/DNV colleagues to validate the processes. Figure 19 presents the derived workflow representation of the simple process as it is now, and Figure 21 presents the workflow representation with EMERALD support.

We first present the simple process and the corresponding workflow presentation covering the processes as they are now. Then, we present the simple process and the elaborated workflow representation as it would look like using the EMERALD solution.

4.2.5.1 Simple Process without EMERALD support

An audit process consists of the following six phases:

- **Phase 1 – Initiating & Preparation** (Figure 18, Phase 1): In this phase, the scope of the audit is defined. This includes the technologies involved, the number of people and locations in scope, and the specific services to be audited. Additionally, this phase includes the document review. Thus, the auditor requests documentation and possibly a self-assessment form from the customer. This documentation includes information about the technologies used, policies, configurations, and other relevant details).
- **Phase 2 – Audit Activities & Phase 3 – Technical Testing** (Figure 18, Phase 2, Phase 3): The audit activities and technical testing are closely interwoven and cannot be separated. The audit activities consist of several steps:
    - Opening the meeting: In the initial meeting relevant practicalities and logistics for the audit are discussed and determined.
    - Document review: Auditors review the documentation provided by the customer to gain an understanding of the respective policies and technologies.
    - Audit workshops: In these workshops, the auditors interact with the customer and conduct interviews and observations to gather information, observe configurations, processes and evidence related to the audit scope.

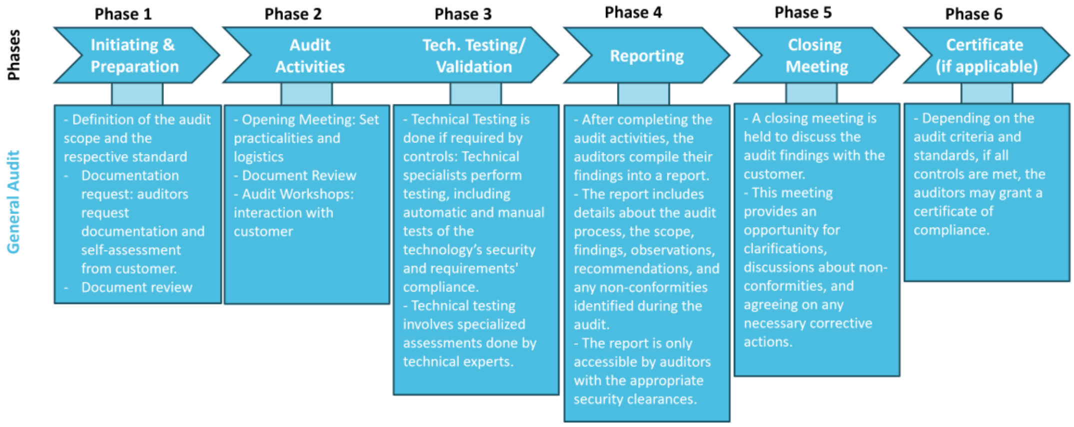
  Technical experts perform specialized assessments including:

    - Automated tools: Utilizing tools like “Nessus” for automated vulnerability scanning and reporting.
    - Manual analysis: Reviewing configurations manually to ensure security and compliance.
    - Validation: Further analysing results from automated tools to provide context and ensure alignment with audit requirements.

- **Phase 4 – Reporting** (Figure 18, Phase 4): After completing the audit activities, the auditors compile their findings into a report. This report typically includes details about the audit process, scope, findings, observations, recommendations, and any non-conformities identified during the audit. These reports contain high-risk and very sensitive information; therefore, it must be ensured that these reports are only accessible by auditors with the appropriate security clearances.

- **Phase 5 – Closing Meeting** (Figure 18, Phase 5): A closing meeting is held to discuss the audit findings and observations with the customer. This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions.

- **Phase 6 – Certificate** (if applicable) (Figure 18, Phase 6): Depending on the audit criteria and standards, if all controls are met, the auditors may grant a certificate of compliance or conformance to the customer.



- Definition of the audit scope and the respective standard
- Documentation request: auditors request documentation and self-assessment from customer.
- Document review

- Opening Meeting: Set practicalities and logistics
- Document Review
- Audit Workshops: interaction with customer

- Technical Testing is done if required by controls: Technical specialists perform testing, including automatic and manual tests of the technology's security and requirements' compliance.
- Technical testing involves specialized assessments done by technical experts.

- After completing the audit activities, the auditors compile their findings into a report.
- The report includes details about the audit process, the scope, findings, observations, recommendations, and any non-conformities identified during the audit.
- The report is only accessible by auditors with the appropriate security clearances.

- A closing meeting is held to discuss the audit findings with the customer.
- This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions.

- Depending on the audit criteria and standards, if all controls are met, the auditors may grant a certificate of compliance.

Figure 18. NIXU/DNV – Simple process representation without EMERALD support

4.2.5.2 Workflow Representation of the Process without EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from NIXU/DNV, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 19.

- **Phase 1: Initiating and Preparation** (Figure 19, Phase 1)**:**
  - Audit scope: The auditor and the customer define the audit scope together.
  - Documentation & self-assessment form: The auditor asks the customer for documentation and a filled-in self-assessment form.
- **Phase 2: Audit Activities & Phase 3: Technical Testing/Validation** (Figure 19, Phase 2 & 3):
  - Audit meeting: The auditors open the meeting and set up the practicalities and logistics. The auditors review the documentation.
  - Check controls: The auditors need to check all technical and organisational controls.
    - Organisational controls: For the organisational controls, the auditors conduct workshops at the customers' site to interact with the customers.
    - Technical controls: Technical auditor and specialists perform testing including automatic and manual tests of the technology to be audited. Technical testing involves specialised assessments done by technical specialists.
- **Phase 4: Reporting** (Figure 19, Phase 4):
  - Report: After the auditors have completed the audit, they compile their findings into a report. The report includes details about the audit process, the scope, findings, observations, recommendations, and any non-conformities identified during the audit. Such a report is only accessible by auditors with the appropriate security clearance.

- **Phase 5: Closing the meeting** (Figure 19, Phase 5)**:**
  - Closing meeting: The auditors hold a closing meeting with the customers to discuss the audit findings. This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions.
- **Phase 6: Certificate** (Figure 19, Phase 6)**:**
  - Certification: Depending on the audit criteria and standard and if all controls have been met, the auditors may grant a certificate of compliance.

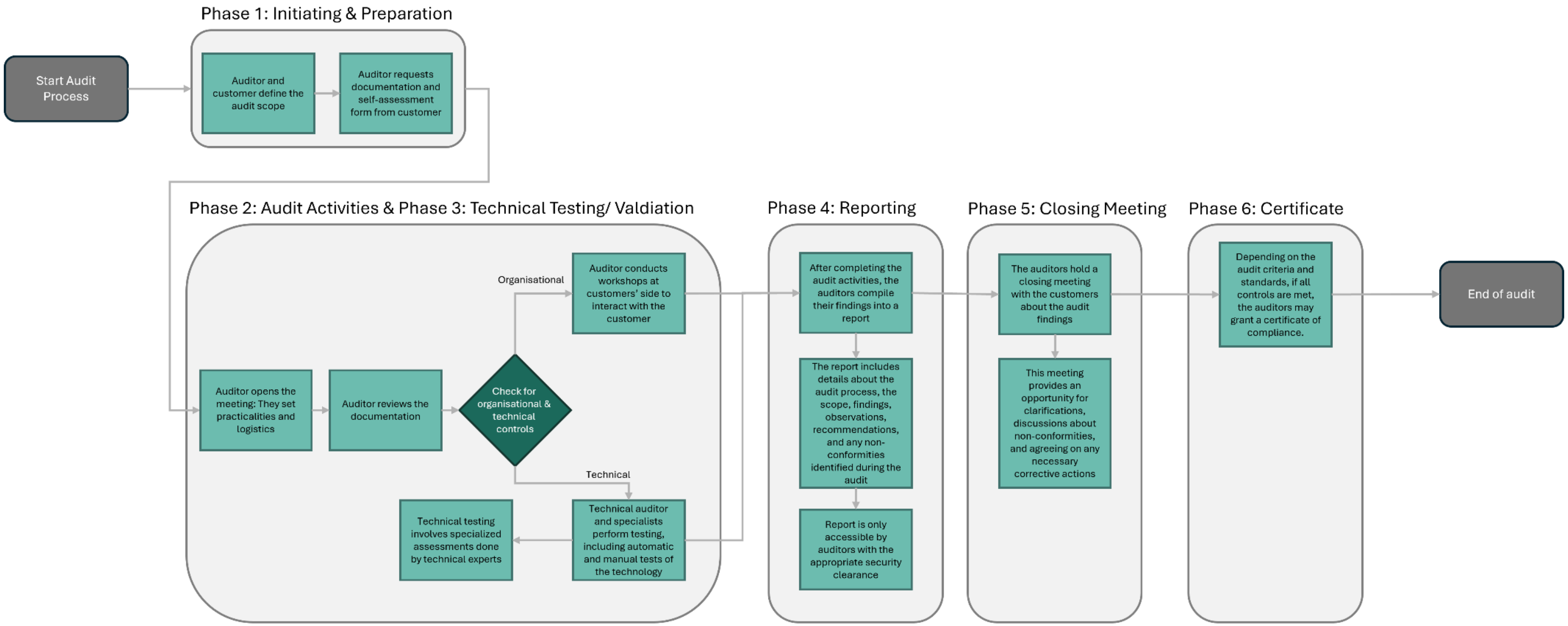

Phase 1: Initiating & Preparation
Start Audit Process
Auditor and customer define the audit scope
Auditor requests documentation and self-assessment form from customer
Phase 2: Audit Activities & Phase 3: Technical Testing/ Valdiation
Auditor opens the meeting: They set practicalities and logistics
Auditor reviews the documentation
Check for organisational & technical controls
Organisational
Auditor conducts workshops at customers' side to interact with the customer
Technical
Technical auditor and specialists perform testing, including automatic and manual tests of the technology
Technical testing involves specialized assessments done by technical experts
Phase 4: Reporting
After completing the audit activities, the auditors compile their findings into a report
The report includes details about the audit process, the scope, findings, observations, recommendations, and any non-conformities identified during the audit
Report is only accessible by auditors with the appropriate security clearance
Phase 5: Closing Meeting
The auditors hold a closing meeting with the customers about the audit findings
This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions
Phase 6: Certificate
Depending on the audit criteria and standards, if all controls are met, the auditors may grant a certificate of compliance.
End of audit

Figure 19. NIXU/DNV – Workflow Representation without EMERALD support

4.2.5.3 Simple Process with EMERALD support

For each of the six phases mentioned above in the audit process, we have derived some ideas on how the audit process of cloud solutions could be supported by the EMERALD UI, as shown in Figure 20:

- **Phase 1 – Initiating & Preparation** (Figure 20, Phase 1): EMERALD could support this phase as follows:
  - Audit scope: The audit scope determines the scope of the audit in relation to cloud services and the respective standard and depends strongly on the customers' domain. EMERALD UI could offer a list of scopes tailored to the partners' cloud solutions.
  - Self-assessment questionnaire: The EMERALD UI can offer a self-assessment questionnaire for EUCS for the pilots that allows them to assess their status regarding the fulfilment of the controls with evidence. The EMERALD UI can support the export of the self-assessment questionnaire in the form of a report that could be provided to the auditors.
- **Phase 2 – Audit Activities & Phase 3 – Technical Testing** (Figure 20, Phase 2 & Phase 3): EMERALD could support both phases as follows:
  - Evidence: Show organisational and technical evidence and their fulfilment regarding the standard and respective controls.
  - Manual verification: Manual verification of controls remains crucial for ensuring accuracy – this could also benefit the auditors.
  - Transparency: The auditor needs to trust the EMERALD technology, which can be ensured by transparency. Thereby, the EMERALD UI could show and explain how technical evidence was created.
  - Metrics: EMERALD UI should offer the possibility to show how the metrics set for the controls are validated. EMERALD UI should present an overview of the controls and their respective metrics.
  - Technical support: Technical support for validating evidence could increase the sample size used during the audit process (more samples could be validated in the same audit time).
- **Phase 4 – Reporting** (Figure 20, Phase 4): EMERALD could support both phases as follows:
  - Audit report generation: EMERALD UI could offer the possibility to download all controls and the respective evidence in form of a report that is accepted by the auditors and the auditing company.
  - Different report types: Depending on the requirements of the auditors, the report could be created using different types including Excel, PDF, word document, etc.

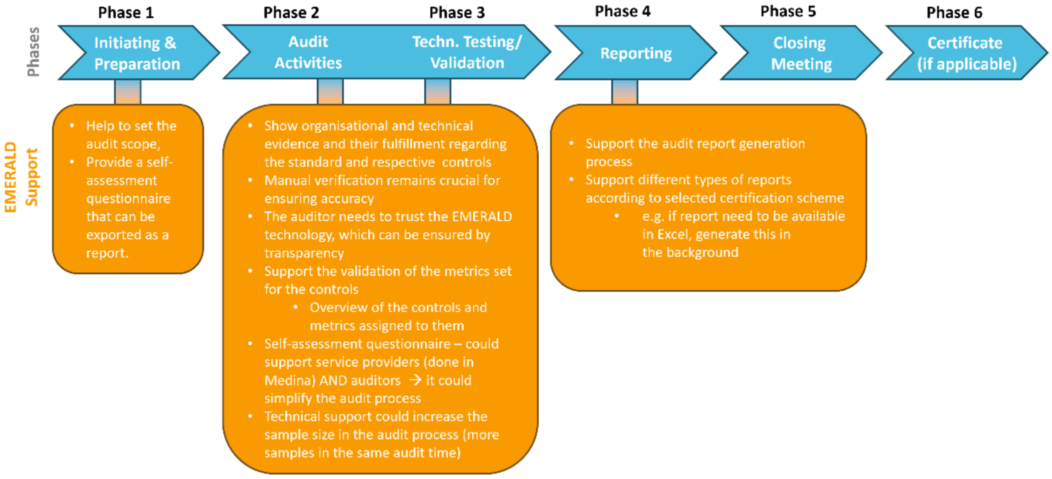

Phases
Phase 1
Initiating & Preparation
Phase 2
Audit Activities
Phase 3
Techn. Testing/ Validation
Phase 4
Reporting
Phase 5
Closing Meeting
Phase 6
Certificate (if applicable)
EMERALD Support
• Help to set the audit scope,
• Provide a self-assessment questionnaire that can be exported as a report.
• Show organisational and technical evidence and their fulfillment regarding the standard and respective controls
• Manual verification remains crucial for ensuring accuracy
• The auditor needs to trust the EMERALD technology, which can be ensured by transparency
• Support the validation of the metrics set for the controls
• Overview of the controls and metrics assigned to them
• Self-assessment questionnaire – could support service providers (done in Medina) AND auditors → it could simplify the audit process
• Technical support could increase the sample size in the audit process (more samples in the same audit time)
• Support the audit report generation process
• Support different types of reports according to selected certification scheme
• e.g. if report need to be available in Excel, generate this in the background

Figure 20. NIXU/DNV – Simple process representation with EMERALD support

4.2.5.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. This representation was again discussed with the colleagues from NIXU/DNV, to investigate, if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 21.

- **Phase 1: Initiating and Preparation** (Figure 21, Phase 1)**:**
  - Audit scope: The auditor and the customer define the audit scope together.
  - Documentation & self-assessment form: The auditor asks the customer for documentation and a filled-in self-assessment form.
  - EMERALD support: The EMERALD UI can provide the policy documents (if uploaded in EMERALD) and the self-assessment form. Both can be accessed by the auditors.
- **Phase 2: Audit Activities & Phase 3: Technical Testing/Validation** (Figure 21, Phase 2 & 3):
  - Audit meeting: The auditors open the meeting and set up the practicalities and logistics. The auditors review the documentation. The auditors can use EMERALD to check the different assessment results for all controls.
  - Check controls: The auditors need to check all technical and organisational controls.
    - Audit scope: Auditors can use EMERALD to review the organisational and technical controls and their fulfilment regarding the standard in the respective “Audit scope”. The auditor can review the (organisational) documentation using EMERALD. The technical auditor can use EMERALD to review the technical assessment results.
    - Certification scheme: Auditors can use EMERALD to validate the metrics set for the controls of a scheme. It provides an overview of the controls, and the metrics assigned to them. “Security Center” → “Certification Schemes”
    - Self-assessment form: EMERALD provides a self-assessment questionnaire for EUCS, which the customers fill in. Auditors can access this questionnaire to simplify the audit process.
  - Auditor conducts workshops on the customers’ side to interact with the customer and use EMERALD as a baseline.
- **Phase 4: Reporting** (Figure 21, Phase 4):
  - Report: After the auditors have completed the audit, they compile their findings into a report. The report includes details about the audit process, the scope, findings,

observations, recommendations, and any non-conformities identified during the audit. Such a report is only accessible by auditors with the appropriate security clearance.
    - Report generation with EMERALD: Auditors can use EMERALD to create the report. EMERALD provides different reports according to the selected certification scheme; reports should be generated in different formats such as .xlsx, docx or pdf.
- **Phase 5: Closing the meeting** (Figure 21 and Figure 19, Phase 5)**:**
    - Closing meeting: The auditors hold a closing meeting with the customers to discuss the audit findings. This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions. The auditors can use EMERALD to guide the discussions about the individual controls and assessment results.
- **Phase 6: Certificate** (Figure 21, Phase 6)**:**
    - Certification: Depending on the audit criteria and standard and if all controls have been met, the auditors may grant a certificate of compliance. EMERALD does not support this step.

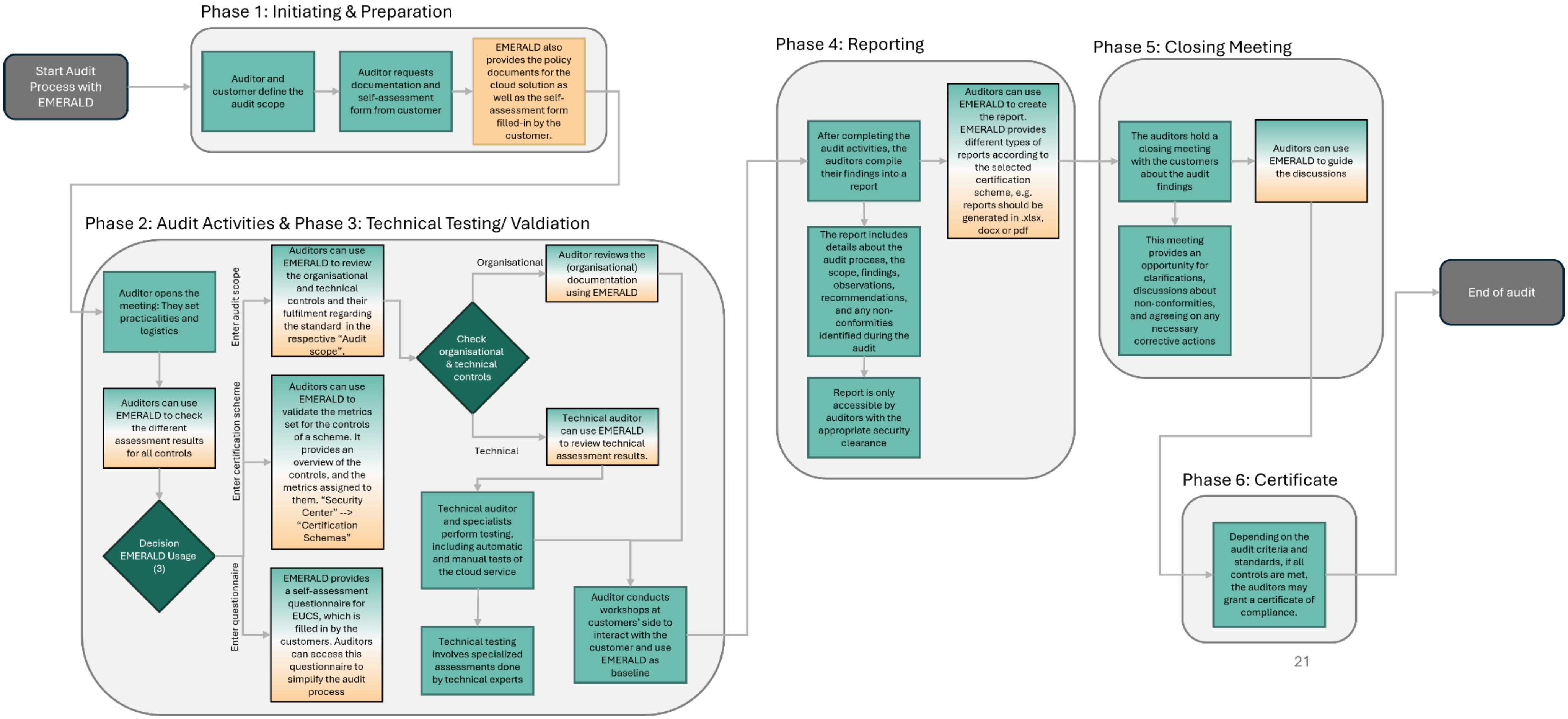

Start Audit Process with EMERALD
Phase 1: Initiating & Preparation
Auditor and customer define the audit scope
Auditor requests documentation and self-assessment form from customer
EMERALD also provides the policy documents for the cloud solution as well as the self-assessment form filled-in by the customer.
Phase 2: Audit Activities & Phase 3: Technical Testing/ Valdiation
Auditor opens the meeting: They set practicalities and logistics
Auditors can use EMERALD to check the different assessment results for all controls
Decision EMERALD Usage (3)
Enter audit scope
Enter certification scheme
Enter questionnaire
Auditors can use EMERALD to review the organisational and technical controls and their fulfilment regarding the standard in the respective "Audit scope".
Auditors can use EMERALD to validate the metrics set for the controls of a scheme. It provides an overview of the controls, and the metrics assigned to them. "Security Center" --> "Certification Schemes"
EMERALD provides a self-assessment questionnaire for EUCS, which is filled in by the customers. Auditors can access this questionnaire to simplify the audit process
Check organisational & technical controls
Organisational
Technical
Auditor reviews the (organisational) documentation using EMERALD
Technical auditor can use EMERALD to review technical assessment results.
Technical auditor and specialists perform testing, including automatic and manual tests of the cloud service
Technical testing involves specialized assessments done by technical experts
Auditor conducts workshops at customers' side to interact with the customer and use EMERALD as baseline
Phase 4: Reporting
After completing the audit activities, the auditors compile their findings into a report
The report includes details about the audit process, the scope, findings, observations, recommendations, and any non-conformities identified during the audit
Report is only accessible by auditors with the appropriate security clearance
Auditors can use EMERALD to create the report. EMERALD provides different types of reports according to the selected certification scheme, e.g. reports should be generated in .xlsx, docx or pdf
Phase 5: Closing Meeting
The auditors hold a closing meeting with the customers about the audit findings
This meeting provides an opportunity for clarifications, discussions about non-conformities, and agreeing on any necessary corrective actions
Auditors can use EMERALD to guide the discussions
End of audit
Phase 6: Certificate
Depending on the audit criteria and standards, if all controls are met, the auditors may grant a certificate of compliance.
21

Figure 21. NIXU/DNV - Workflow Representation with EMERALD support

4.2.6 Compliance Manager (NIXU/DNV)

We conducted an interview with a compliance manager from NIXU/DNV which was organised by the NIXU/DNV EMERALD project manager. Additionally, after having analysed the results, we conducted a focus group with the responsible compliance manager and the NIXU/DNV EMERALD project manager to get input and feedback about the derived simple processes. Figure 22 presents the simple process of an audit preparation process as it is now, while Figure 24 presents the simple process enhanced with the EMERALD support.

After having transformed the simple process representation into a workshop representation without and with EMERALD support, we conducted a workshop with the NIXU/DNV colleagues to validate the processes. Figure 23 presents the derived workflow representation of the simple process as it is now, and Figure 25 presents the workflow representation with EMERALD support.

We first present the simple process and the corresponding workflow presentation covering the processes as they are now. Then, we present the simple process and the elaborated workflow representation as it would look like using the EMERALD solution.

4.2.6.1 Simple Process without EMERALD Support

The simple process without EMERALD support consists of the following five phases:

- **Phase 1 - Preparation and Setup** (Figure 22, Phase 1): Phase 1 is the setup, including establishing the compliance framework, setting up the continuous compliance monitoring process, and informing all relevant stakeholders.
- **Phase 2 - Monitoring and Identification** (Figure 22, Phase 2): In this phase, the continuous monitoring and identification of the controls and the respective evidence should take place. If some deviations or non-conformities are identified, the relevant stakeholders need to be informed.
- **Phase 3 - Evaluation & Decision Making** (Figure 22, Phase 3): In this phase, identified deviations or non-conformities need to be evaluated, and a decision must be taken if and how corrective actions will be taken.
- **Phase 4 - Corrective Action Planning & Implementation** (Figure 22, Phase 4): If it has been decided to take corrective actions, these actions must be planned, pursued, and implemented.
- **Phase 5 – Reporting** (Figure 22, Phase 5): In this phase, all activities done regarding the controls and their evidence, as well as all information related to corrective actions, need to be summarised in reports to be available for the audit.

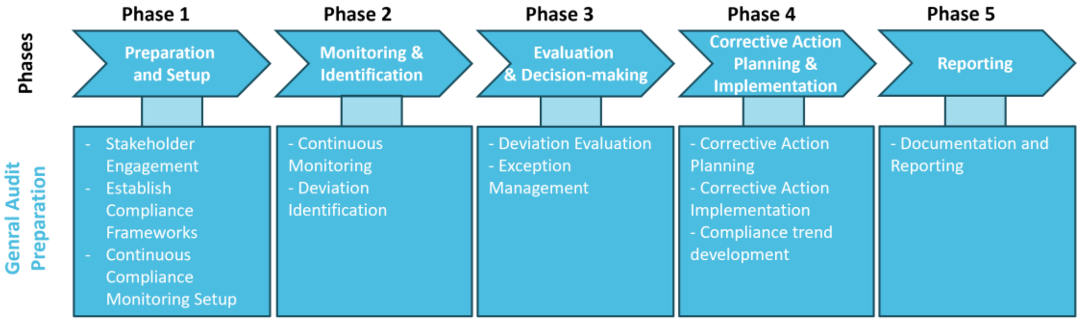

Phases
Genral Audit Preparation
Phase 1
Preparation and Setup
- Stakeholder Engagement
- Establish Compliance Frameworks
- Continuous Compliance Monitoring Setup
Phase 2
Monitoring & Identification
- Continuous Monitoring
- Deviation Identification
Phase 3
Evaluation & Decision-making
- Deviation Evaluation
- Exception Management
Phase 4
Corrective Action Planning & Implementation
- Corrective Action Planning
- Corrective Action Implementation
- Compliance trend development
Phase 5
Reporting
- Documentation and Reporting

Figure 22. NIXU/DNV CM – Simple process representation without EMERALD support

4.2.6.2 Workflow Representation of the Process without EMERALD Support

In the next step, we transferred the simple process representation into a detailed workflow representation. While the workflow follows a continuous compliance management process with a loop, the loop itself is not explicitly depicted in the representation. This representation was again discussed with the colleagues from NIXU/DNV, to investigate if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 23.

- **Phase 1 - Preparation & Setup** (Figure 23, Phase 1):
    - Stakeholder Engagement: The CM identifies key stakeholders, including technical architects, security managers, and compliance managers, and establishes regular meeting schedules for setting up the audit preparation process.
    - Controls: The CM identifies external and internal requirements to select suitable compliance frameworks in relation to the cloud service that will be audited.
    - Establish Compliance Frameworks: The CM determines the compliance frameworks relevant to the organisation, e.g. ISO 27001, SOC, and GDPR.
    - Continuous Compliance Monitoring Setup: The CM sets up all respective systems and the governance model for continuous monitoring of the compliance status, including tools and dashboards, etc.
- **Phase 2 - Monitoring and Identification** (Figure 23, Phase 2):
    - Continuous Monitoring: The CM collects reports and dashboard information regularly to monitor compliance status against established frameworks.
    - Deviation Identification: The CM uses tools and dashboards (e.g., Excel for tracking, manual processes, leverage specialized compliance monitoring tools like Azure's internal tools[6]) to identify deviations from compliance controls.
- **Phase 3 - Evaluation & Decision Making** (Figure 23, Phase 3):
    - Deviation Evaluation: The CM evaluates identified deviations to determine their acceptability or if corrective actions are required.
    - Exception Management and Risk Identification: Exception and risk management are closely connected and iterated processes.
    - Exception Management: Setting exceptions - when during evaluation something is found to be not compliant but might be acceptable in a specific environment or under distinctive conditions and thus, no corrective actions are needed there, exceptions are defined and set.
    - Risk Identification: For each identified exception, the risk is assessed and is either accepted and reported or corrective steps will be taken.
- **Phase 4 - Corrective Action Planning & Implementation** (Figure 23, Phase 4):
    - Corrective Action Planning: The CM plans corrective actions for identified deviations and assigns responsibilities to relevant personnel.
    - Corrective Action Implementation: The CM and the relevant personnel implement corrective actions and address technical issues and policy-related concerns.
- **Phase 5 – Reporting** (Figure 23, Phase 5):
    - Compliance Trend Development: The CM pursues the compliance trend development of the controls and does manual reporting.
    - Documentation and Reporting: The CM summarises discussions and reviews information before presenting it in the respective audits.

[6] https://azure.microsoft.com/

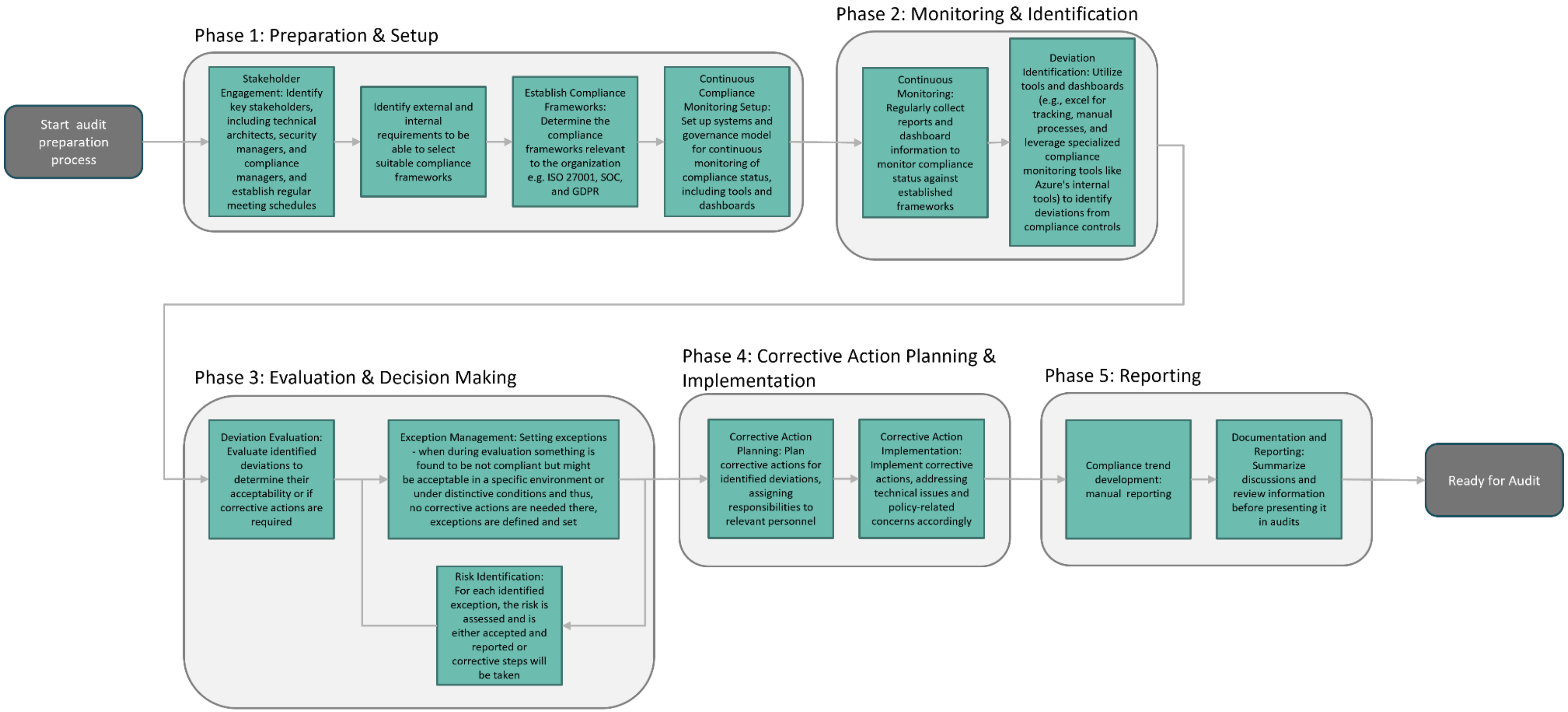

Start audit preparation process
Phase 1: Preparation & Setup
Stakeholder Engagement: Identify key stakeholders, including technical architects, security managers, and compliance managers, and establish regular meeting schedules
Identify external and internal requirements to be able to select suitable compliance frameworks
Establish Compliance Frameworks: Determine the compliance frameworks relevant to the organization e.g. ISO 27001, SOC, and GDPR
Continuous Compliance Monitoring Setup: Set up systems and governance model for continuous monitoring of compliance status, including tools and dashboards
Phase 2: Monitoring & Identification
Continuous Monitoring: Regularly collect reports and dashboard information to monitor compliance status against established frameworks
Deviation Identification: Utilize tools and dashboards (e.g., excel for tracking, manual processes, and leverage specialized compliance monitoring tools like Azure's internal tools) to identify deviations from compliance controls
Phase 3: Evaluation & Decision Making
Deviation Evaluation: Evaluate identified deviations to determine their acceptability or if corrective actions are required
Exception Management: Setting exceptions - when during evaluation something is found to be not compliant but might be acceptable in a specific environment or under distinctive conditions and thus, no corrective actions are needed there, exceptions are defined and set
Risk Identification: For each identified exception, the risk is assessed and is either accepted and reported or corrective steps will be taken
Phase 4: Corrective Action Planning & Implementation
Corrective Action Planning: Plan corrective actions for identified deviations, assigning responsibilities to relevant personnel
Corrective Action Implementation: Implement corrective actions, addressing technical issues and policy-related concerns accordingly
Phase 5: Reporting
Compliance trend development: manual reporting
Documentation and Reporting: Summarize discussions and review information before presenting it in audits
Ready for Audit

Figure 23. NIXU/DNV CM – Workflow Representation without EMERALD support

4.2.6.3 Simple Process with EMERALD Support

For each of the five phases mentioned above in the simple process of the audit preparation, we have derived some ideas on how the audit preparation process of cloud solutions could be supported by the EMERALD UI, as shown in Figure 24.

- **Phase 1 - Preparation & Setup** (Figure 24, Step 1)**:** EMERALD can provide support for the following tasks:
  - Setup: EMERALD can support the setup of the respective compliance framework, standards, or certification schemes.
  - Cloud service: EMERALD can support the selection of the cloud solution to be audited.
  - Continuous monitoring setup: EMERALD can support the definition of specific parameters for the continuous monitoring of controls and evidence.
  - Tasks: EMERALD can support task management throughout the audit preparation process.

- **Phase 2 - Monitoring and Identification & Phase 3 - Evaluation & Decision Making** (Figure 24, Step 2 – Step 3): EMERALD can provide support for the following tasks:
  - Continuous monitoring: EMERALD can help to support continuous monitoring of the cloud service according to different parameters. The EMERALD UI should provide a dashboard that integrates data from different targets of evaluation to have all data and critical deviations in one glance. Thereby, EMERALD should show possible deviations or non-conformities found.
  - Log historical data (e.g., when was a deviation, how was this solved, etc.): Additionally, the EMERALD UI should provide activity log data in the form of a history to make all changes of controls or metrics visible, traceable and transparent.
- **Phase 4 - Corrective Action Planning & Implementation** (Figure 24, Step 4): EMERALD can provide support for the following tasks:
  - Corrective action management: EMERALD should allow the possibility of noting down decisions made regarding the implementation of corrective actions. This includes, for example, having a list of pending tasks that allows to plan and follow up the implementation of the corrective actions.
  - History: EMERALD can collect, save and visualise a history log file of all tasks and activities performed within the EMERALD UI.

- **Phase 5 – Reporting** (Figure 24, Step 5): EMERALD can provide support for the following tasks:
  - Controls and evidence: EMERALD could offer the possibility to create a document covering all information about the controls and metrics and the respective assessment results and evidence.
  - Support during audits: EMERALD could provide the possibility to download different types of reports to support the audit preparation process (e.g., different documents in different formats like Excel sheets, Word Files, etc.).

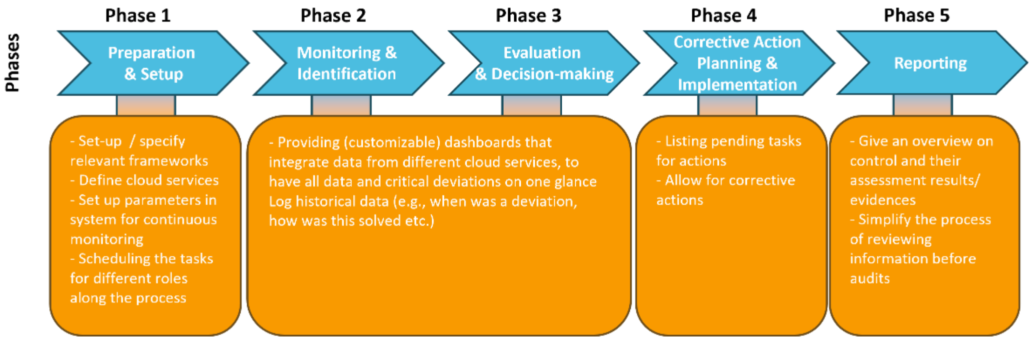

Phases
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Preparation & Setup
Monitoring & Identification
Evaluation & Decision-making
Corrective Action Planning & Implementation
Reporting
- Set-up / specify relevant frameworks
- Define cloud services
- Set up parameters in system for continuous monitoring
- Scheduling the tasks for different roles along the process
- Providing (customizable) dashboards that integrate data from different cloud services, to have all data and critical deviations on one glance Log historical data (e.g., when was a deviation, how was this solved etc.)
- Listing pending tasks for actions
- Allow for corrective actions
- Give an overview on control and their assessment results/ evidences
- Simplify the process of reviewing information before audits

Figure 24. NIXU/DNV CM – Simple process representation with EMERALD support

4.2.6.4 Workflow Representation of the Process with EMERALD support

In the next step, we transferred the simple process representation into a detailed workflow representation. While the workflow follows a continuous compliance management process with a loop, the loop itself is not explicitly depicted in the representation. This representation was again discussed with the colleagues from NIXU/DNV, to investigate, if the workflow representation is correct. After some minor improvements, the resulting workflow process is presented in Figure 25.

- **Phase 1 - Preparation & Setup** (Figure 25, Step 1):
  - Stakeholder engagement: The CM identifies key stakeholders, including technical architects, security managers, and compliance managers, and establishes regular meeting schedules.
  - Controls: The CM identifies external and internal requirements to select suitable compliance frameworks in relation to the cloud service that will be audited.
  - Establish compliance frameworks: The CM determines the compliance frameworks relevant to the organisation, e.g., ISO 27001, SOC, and GDPR.
  - Continuous compliance monitoring setup: CM prepares and uploads the certification scheme or works with an existing scheme in EMERALD.
  - The EMERALD UI makes available all controls and automatically assigns metrics to controls.
- **Phase 2 - Monitoring and Identification** (Figure 25, Phase 2):
  - Continuous monitoring: CM collects reports and dashboard information regularly to monitor compliance status against established frameworks.
  - Deviation identification: CM sets up a target of evaluation and audit scope in EMERALD. CM uses the different views and functionalities of the EMERALD UI to access controls that are noncompliant.
  - EMERALD: EMERALD tries to automatically extract evidence for all controls and their metrics.
  - EMERALD: EMERALD provides a list of all controls, metrics, and the respective assessment results for each audit scope.
- **Phase 3 - Evaluation and Decision Making & Phase 4 – Corrective Action Planning & Implementation** (Figure 25, Phase 3 & 4):
  - Check controls: CM manually checks all assessment result for all controls and metrics in EMERALD and can filter for all controls that are still marked as “open”.
  - If all controls/metrics are compliant or not open anymore, the CM continues with Phase 5.
  - Check assessment results: The CM checks for each control and metrics and the assessment results/evidence in EMERALD.

  - Deviation evaluation: The CM identifies deviations to determine their acceptability or if corrective actions are required. Depending on what is necessary, the CM either cares for the exception and risk management or with the implementation of corrective actions.
  - Exception management and risk identification: Exception and risk management are closely connected and iterated processes.
    - Exception management: Setting exceptions - when during evaluation something is found to be not compliant but might be acceptable in a specific environment or under distinctive conditions and thus, no corrective actions are needed there, exceptions are defined and set.
    - Risk identification: For each identified exception, the risk is assessed and is either accepted and reported or corrective, steps will be taken.
  - Corrective action planning:
    - The CM plans corrective actions for the identified deviations.
    - Corrective action planning: CM assigns controls or metrics to relevant personnel.
    - Check assessment result: Assigned person checks the assessment results of the assigned control/metric provided in EMERALD.
    - Corrective action implementation: The person implements the corrective actions, addressing technical issues and policy-related concerns accordingly.
    - Person assigns the control/metric in EMERALD back to the CM.
- **Phase 5 – Reporting** (Figure 25, Phase 5):
  - Compliance trend development: The CM pursues the compliance trend development of the controls and does manual reporting.
  - Documentation and reporting: The CM summarizes discussions and reviews information before presenting it in the respective audits.

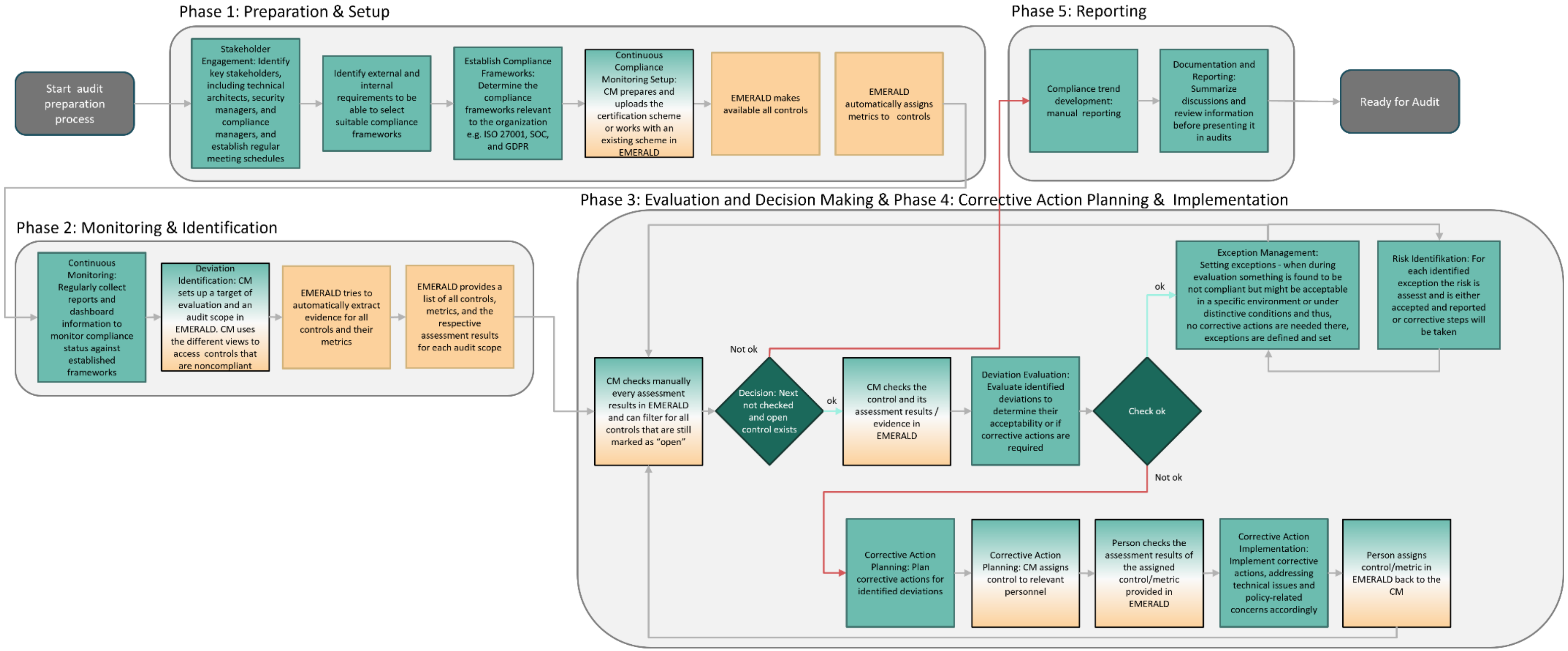

Phase 1: Preparation & Setup
Start audit preparation process
Stakeholder Engagement: Identify key stakeholders, including technical architects, security managers, and compliance managers, and establish regular meeting schedules
Identify external and internal requirements to be able to select suitable compliance frameworks
Establish Compliance Frameworks: Determine the compliance frameworks relevant to the organization e.g. ISO 27001, SOC, and GDPR
Continuous Compliance Monitoring Setup: CM prepares and uploads the certification scheme or works with an existing scheme in EMERALD
EMERALD makes available all controls
EMERALD automatically assigns metrics to controls
Phase 5: Reporting
Compliance trend development: manual reporting
Documentation and Reporting: Summarize discussions and review information before presenting it in audits
Ready for Audit
Phase 2: Monitoring & Identification
Continuous Monitoring: Regularly collect reports and dashboard information to monitor compliance status against established frameworks
Deviation Identification: CM sets up a target of evaluation and an audit scope in EMERALD. CM uses the different views to access controls that are noncompliant
EMERALD tries to automatically extract evidence for all controls and their metrics
EMERALD provides a list of all controls, metrics, and the respective assessment results for each audit scope
Phase 3: Evaluation and Decision Making & Phase 4: Corrective Action Planning & Implementation
CM checks manually every assessment results in EMERALD and can filter for all controls that are still marked as "open"
Not ok
Decision: Next not checked and open control exists
ok
CM checks the control and its assessment results / evidence in EMERALD
Deviation Evaluation: Evaluate identified deviations to determine their acceptability or if corrective actions are required
Check ok
ok
Not ok
Exception Management: Setting exceptions - when during evaluation something is found to be not compliant but might be acceptable in a specific environment or under distinctive conditions and thus, no corrective actions are needed there, exceptions are defined and set
Risk Identifikation: For each identified exception the risk is assesst and is either accepted and reported or corrective steps will be taken
Corrective Action Planning: Plan corrective actions for identified deviations
Corrective Action Planning: CM assigns control to relevant personnel
Person checks the assessment results of the assigned control/metric provided in EMERALD
Corrective Action Implementation: Implement corrective actions, addressing technical issues and policy-related concerns accordingly
Person assigns control/metric in EMERALD back to the CM

Figure 25. NIXU/DNV CM - Workflow Representation with EMERALD support

4.3 Blueprint for introducing EMERALD in audit preparation

In the final step, we integrated key insights and process steps from all four pilot partners and NIXU/DNV, refining them into a universally applicable blueprint for implementing EMERALD in audit preparation and audit execution workflows as presented in Figure 26, Figure 27, and Figure 28. Implementing a universally applicable blueprint for integrating EMERALD into audit preparation processes or using it during audits provides a structured, efficient, and scalable approach, offering several key advantages:

- **Consistency & Standardization** – It ensures a structured and repeatable approach across different organizations, reducing variability in implementation.
- **Efficiency & Time-Saving** – It streamlines audit preparation processes by providing clear guidelines, reducing trial-and-error efforts.
- **Scalability** – Makes it easier to expand EMERALD's adoption across multiple departments, organizations, or industries.
- **Best Practices Integration** – It consolidates lessons learned from various pilot partners and NIXU/DNV, ensuring the approach is based on approaches that are currently in place.
- **Enhanced Collaboration** – It facilitates communication between stakeholders by providing a shared framework and terminology.
- **Flexibility** – While standardized, a well-designed blueprint allows for customization to fit specific organizational needs.
- **Faster Onboarding & Training** – New target users and teams can more easily understand and adopt the system with a clear roadmap.
- **Regulatory Compliance** – It can help align processes with industry standards and regulatory requirements, ensuring smooth audits.

In the following, we provide a detailed overview of the six individual phases of the blueprint. We identify which pilot partners and NIXU/DNV share the same process steps in the phases.

- **Phase 1 – Certification Scheme** (Figure 26, Phase 1):
  - Upload/Use certification scheme: CM uploads a certification scheme or creates a new certification scheme or works with an existing scheme in EMERALD.
  - EMERALD makes available all controls in an easy-to-use way.
  - EMERALD automatically assigns metrics to controls.
- **Phase 2 – Check controls and Metrics** (Figure 26, Phase 2):
  - Check controls: CM checks all automatically assigned metrics to a control.
    - If the check is not ok: CM checks all metrics of a controls and changes them where needed.
    - If the check is ok: CM continues with Phase 3.
- **Phase 3 – Setup target of evaluation and audit scope** (Figure 26, Phase 3):
  - Setup target of evaluation: The CM needs to set up a new target of evaluation; then either the CM or technicians need to install appropriate evidence extractors for the respective cloud service; CM uploads the policy documents in EMERALD.
  - Setup audit scope: The CM sets up a new audit scope by using the newly created target of evaluation and the respective certification scheme, including its controls and the respective metrics.
- **Phase 4 – Audit Scope** (Figure 27, Phase 4):
  - EMERALD tries to automatically extract assessment results and evidence for all controls and their metrics.
  - EMERALD provides a list of all controls/metrics and the respective assessment results.

  - Deviation identification: The CM can browse through all controls/metrics and is able to filter between compliant and noncompliant assessment results in EMERALD. Depending on if there exist controls that need to be checked, the CM has different options on how to proceed in Phase 5.

- **Phase 5 – Check controls and assessment results** (Figure 27, Phase 5):
  - If controls need to be checked: The CM goes to the control/metric and checks the corresponding assessment results/evidence.
    - If the check is ok: Based on the available assessment results (and the domain knowledge of the CM), the CM can set the control/metric in EMERALD to compliant.
    - If the check is not ok: The CM/Person assigns control/metric to another person or a department.
  - Check assessment results: The person checks the assessment results/evidence of the assigned control/metric provided in EMERALD. Depending on the check, the person has four options as follows:
    - Check ok: Based on the available assessment results (and the domain knowledge of the person), the person can set the control/metric to compliant/done in EMERALD and assign the control/metric back to the CM.
    - Check not ok, no assessment result is available: If a control cannot be automatically assessed, the person can add evidence manually (Exception Management). Person assigns the control/metric back to the CM.
    - Check not ok, but the person knows how to solve it: Person implements the measurement for the metrics, sets the control/metric to compliant (Exception Management) and assigns the control/metric back to the CM.
    - Check not ok, and person does not know how to solve it: CM/Person assigns control to another person or a department or back to the CM.
  - If no controls need to be further checked by the CM: CM has checked all controls and documents and consolidates everything for the audit. Then the CM decides how to proceed, e.g., with Phase 6a or Phase 6b or if everything is prepared for the audit.
- **Phase 6a – Reporting** (Figure 28, Phase 6a):
  - EMERALD: EMERALD can help with providing different types of outcomes.
  - Audit report: This document compiled by auditors summarizes the findings of the audit process. It outlines areas of compliance and identifies non-compliance issues.
  - Track record of evidence: A comprehensive record of evidence is gathered and maintained. This report includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation.
  - Compliance status: The audit process determines the compliance status of the service in question. It indicates whether the service meets the established standards, regulations, and risk threshold.
  - Categorization of the service: The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly.
- **Phase 6b – Validation** (Figure 28, Phase 6b): EMERALD can support the compliance manager and the other departments with the following tasks during the verification phase:
  - Validity check: In the final phase of the process, the compliance manager does a validity check, which is a final check that all respective controls are compliant.
  - Filter for controls: To do so the CM goes through all controls again, checks all controls especially those that have been assigned back to the CM or need more discussions.

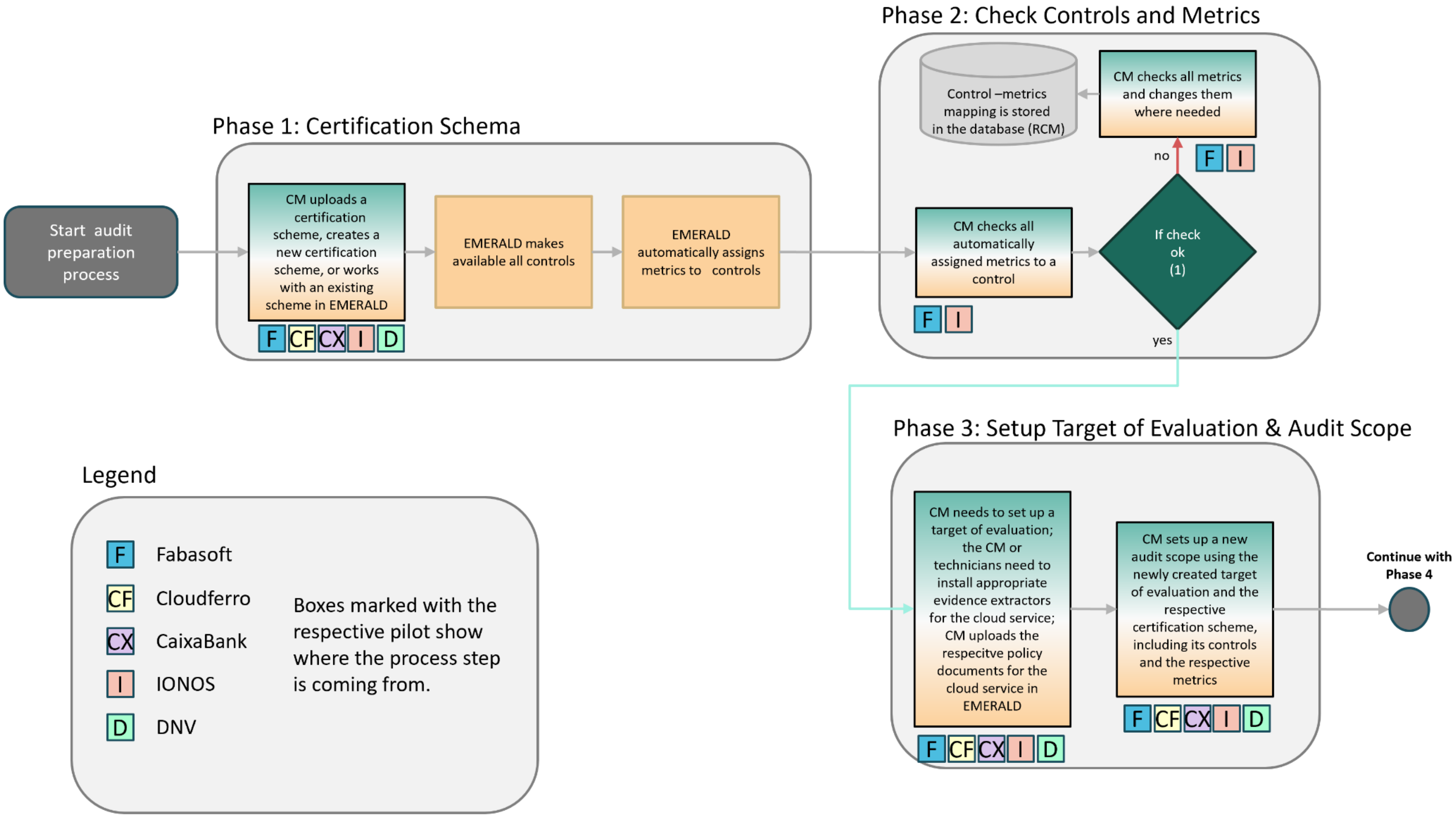

Phase 1: Certification Schema
Phase 2: Check Controls and Metrics
Phase 3: Setup Target of Evaluation & Audit Scope
Start audit preparation process
CM uploads a certification scheme, creates a new certification scheme, or works with an existing scheme in EMERALD
F CF CX I D
EMERALD makes available all controls
EMERALD automatically assigns metrics to controls
CM checks all automatically assigned metrics to a control
F I
If check ok (1)
no
yes
CM checks all metrics and changes them where needed
F I
Control –metrics mapping is stored in the database (RCM)
CM needs to set up a target of evaluation; the CM or technicians need to install appropriate evidence extractors for the cloud service; CM uploads the respecitve policy documents for the cloud service in EMERALD
F CF CX I D
CM sets up a new audit scope using the newly created target of evaluation and the respective certification scheme, including its controls and the respective metrics
F CF CX I D
Continue with Phase 4
Legend
F Fabasoft
CF Cloudferro
CX CaixaBank
I IONOS
D DNV
Boxes marked with the respective pilot show where the process step is coming from.

Figure 26. EMERALD blueprint workflow representation - Part 1

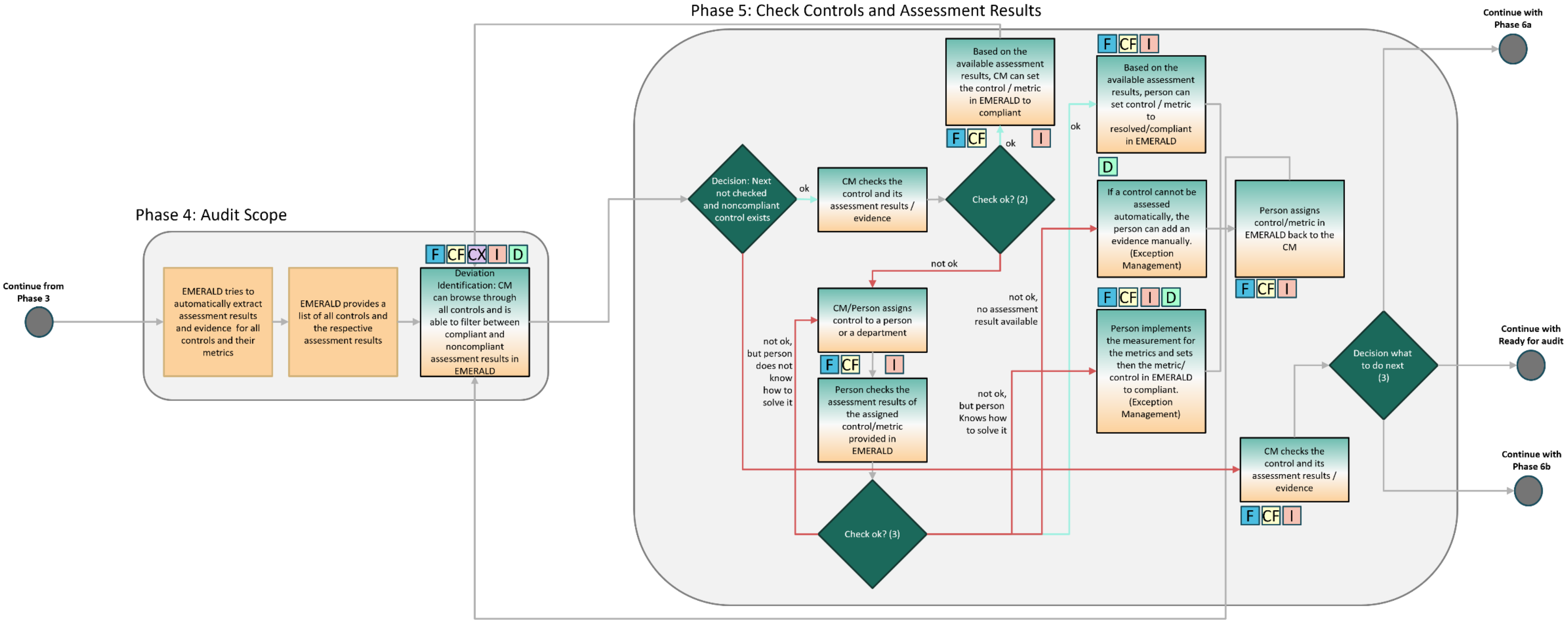

Phase 5: Check Controls and Assessment Results
Continue with Phase 6a
Phase 4: Audit Scope
Continue from Phase 3
EMERALD tries to automatically extract assessment results and evidence for all controls and their metrics
EMERALD provides a list of all controls and the respective assessment results
F CF CX I D
Deviation Identification: CM can browse through all controls and is able to filter between compliant and noncompliant assessment results in EMERALD
Decision: Next not checked and noncompliant control exists
ok
CM checks the control and its assessment results / evidence
Check ok? (2)
ok
Based on the available assessment results, CM can set the control / metric in EMERALD to compliant
F CF
I
F CF I
Based on the available assessment results, person can set control / metric to resolved/compliant in EMERALD
ok
D
If a control cannot be assessed automatically, the person can add an evidence manually. (Exception Management)
Person assigns control/metric in EMERALD back to the CM
F CF I
not ok
CM/Person assigns control to a person or a department
F CF
I
not ok, no assessment result available
F CF I D
Person implements the measurement for the metrics and sets then the metric/ control in EMERALD to compliant. (Exception Management)
not ok, but person does not know how to solve it
Person checks the assessment results of the assigned control/metric provided in EMERALD
not ok, but person Knows how to solve it
Check ok? (3)
Decision what to do next (3)
Continue with Ready for audit
CM checks the control and its assessment results / evidence
F CF I
Continue with Phase 6b

Figure 27. EMERALD blueprint workflow representation – Part 2

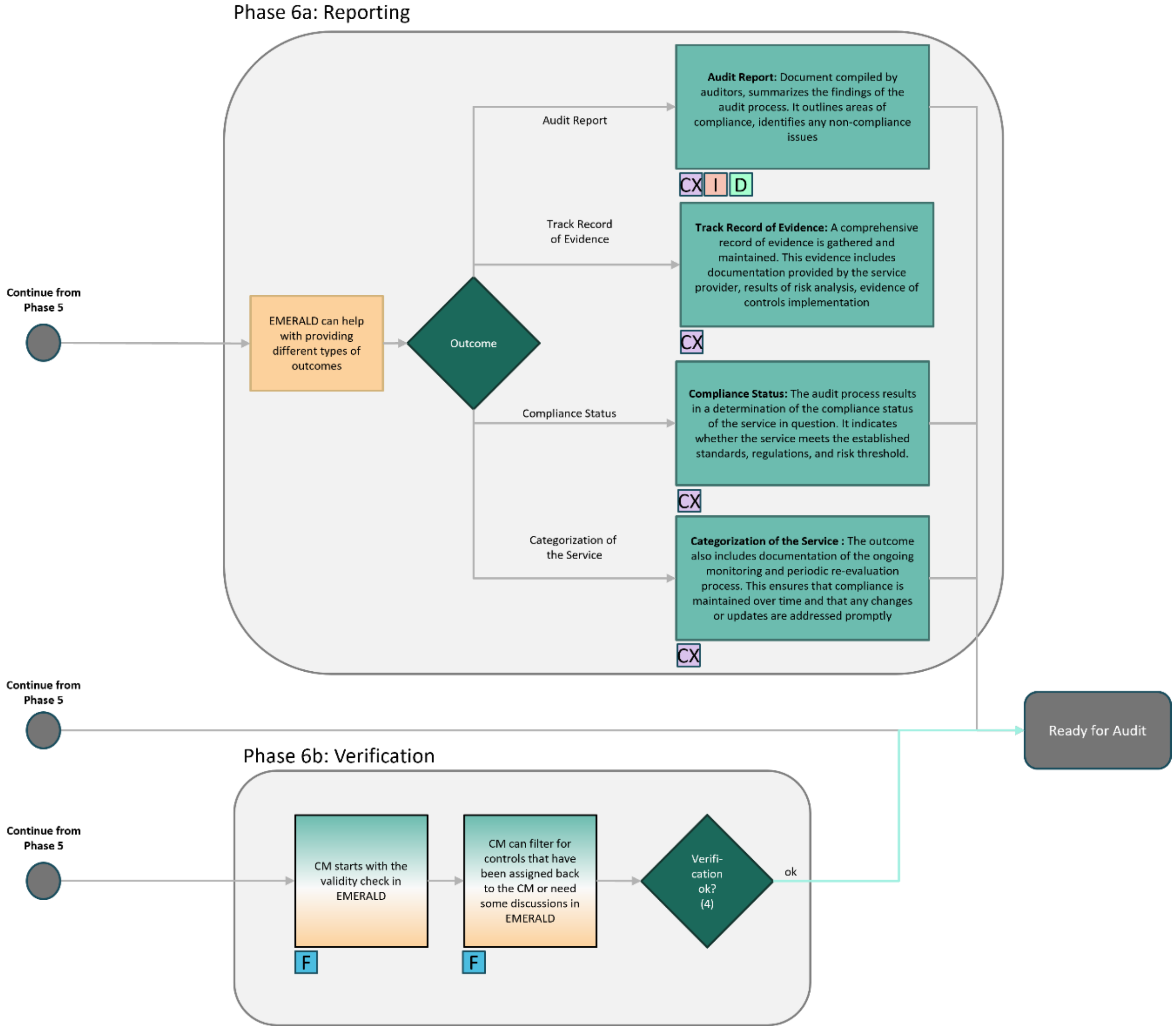

Phase 6a: Reporting
Continue from Phase 5
EMERALD can help with providing different types of outcomes
Outcome
Audit Report
Track Record of Evidence
Compliance Status
Categorization of the Service
Audit Report: Document compiled by auditors, summarizes the findings of the audit process. It outlines areas of compliance, identifies any non-compliance issues
CX I D
Track Record of Evidence: A comprehensive record of evidence is gathered and maintained. This evidence includes documentation provided by the service provider, results of risk analysis, evidence of controls implementation
CX
Compliance Status: The audit process results in a determination of the compliance status of the service in question. It indicates whether the service meets the established standards, regulations, and risk threshold.
CX
Categorization of the Service : The outcome also includes documentation of the ongoing monitoring and periodic re-evaluation process. This ensures that compliance is maintained over time and that any changes or updates are addressed promptly
CX
Continue from Phase 5
Ready for Audit
Phase 6b: Verification
Continue from Phase 5
CM starts with the validity check in EMERALD
F
CM can filter for controls that have been assigned back to the CM or need some discussions in EMERALD
F
Verifi-cation ok? (4)
ok

Figure 28. EMERALD blueprint workflow representation – Part 3

5 Personas, Personas-on-the-go and Scenarios

This section presents the final version of the identified stakeholder personas, developed based on the insights gathered through workshops conducted with pilot partners and NIXU/DNV.

The EMERALD personas can be divided into three different stakeholder groups – compliance stakeholders, technical stakeholders, and auditor stakeholders – as presented in Figure 29.

- **Compliance Stakeholders**: The goal of compliance stakeholders is to prepare for a certification thoroughly; they would like to use the EMERALD framework to set up, manage, and monitor their certifications and enable lean re-certification.
- **Technical Stakeholders**: The goal of the technical stakeholders is to support the management and implementation of the measurement of metrics for controls.
- **Auditor Stakeholders**: The goal of auditors is to use the EMERALD solutions to manage audits, review controls, evidence, and the respective documents, and to create reports on different levels easily.

Goal: The goal of defining these personas is threefold. First, understanding the roles and tasks of compliance managers, auditors, and technical stakeholders is essential for designing a system that effectively supports certification preparation and audit execution. By analysing these personas, we gain a clearer picture of the challenges users face during the audit preparation or audit execution and how they interact with compliance-related processes. Second, these personas are instrumental in shaping the EMERALD UI by identifying the key functionalities needed to support each stakeholder group including the user administration and which user is allowed to do what in EMERALD. Finally, the development of personas contributes to the elicitation of concrete design and system requirements, ensuring that the EMERALD framework is built to accommodate real-world user needs.

To make these personas more accessible, we have developed “personas-on-the-go”, a concise visual summary highlighting key characteristics of each user type. This approach improves accessibility, allowing stakeholder unfamiliar with EMERALD to quickly understand the main user groups without having to go in-depth into the available documentation. It also facilitates fast decision-making, providing clear reference when designing, implementing and refining EMERALD’s features. Additionally, by summarizing the most relevant attributes in an easy-to-understand format, the “personas-on-the-go” enhance communication across the EMERALD consortium and ensures that the system’s technical implementation remains user-centred.

Beyond the personas, corresponding scenarios have been developed to illustrate how different users interact with the system in real-world situations. These scenarios provide essential context, ensuring that EMERALD aligns with actual workflows and user needs. They also help to identify potential usability issues, guiding the refinement of technical features by highlighting pain points and opportunities for improvement. Scenarios serve as a foundation for testing and validation, allowing the EMERALD consortium to access whether EMERALD meets user expectations and regulatory requirements effectively. Throughout the project, some scenarios were adjusted due to technical feasibility or implementation considerations. In cases where discrepancies existed between the textual description and the corresponding figure, the figure was placed directly beneath the scenario description. If no modifications were made, the original figures are included in *APPENDIX B: Original User Scenario Descriptions*.

By generating personas, “personas-on-the-go”, and scenarios, the EMERALD framework provides compliance managers, technical teams, and auditors with a user-centred system that is intuitive, tailored to their specific needs, and aligned with real-world certification and auditing processes.

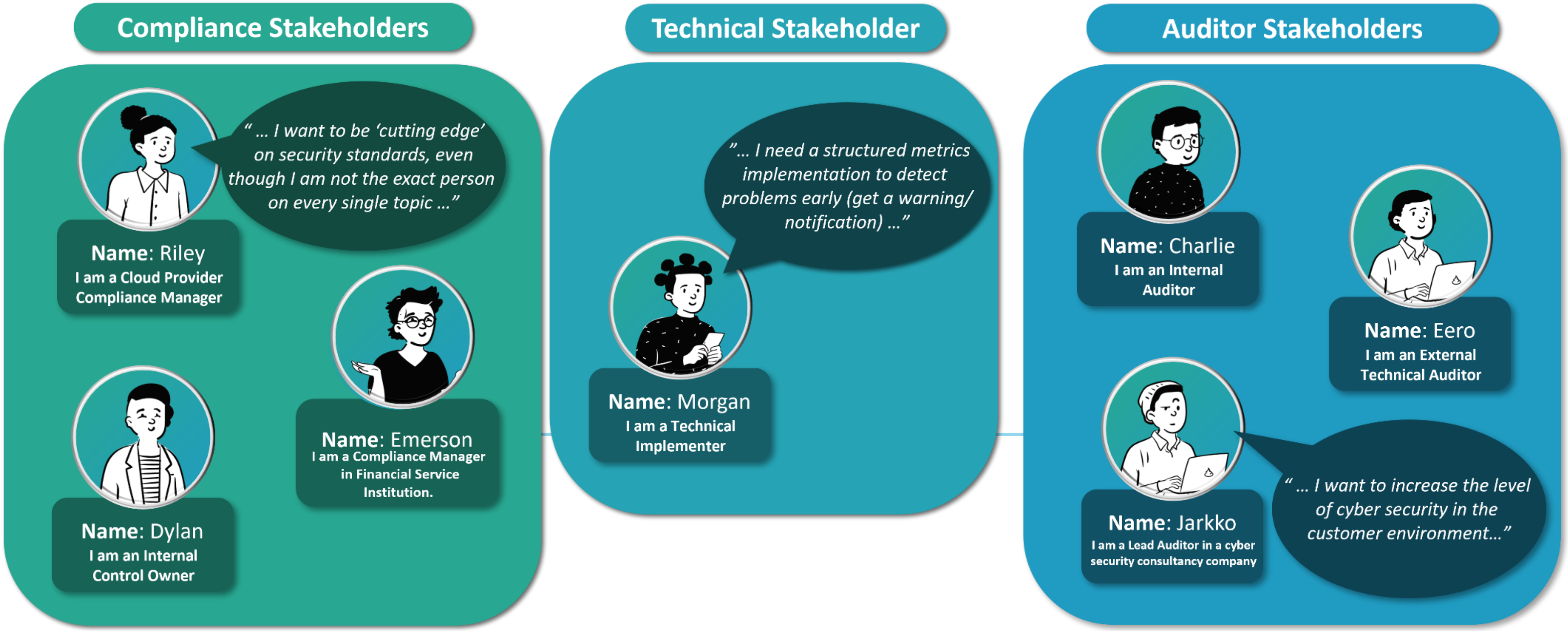
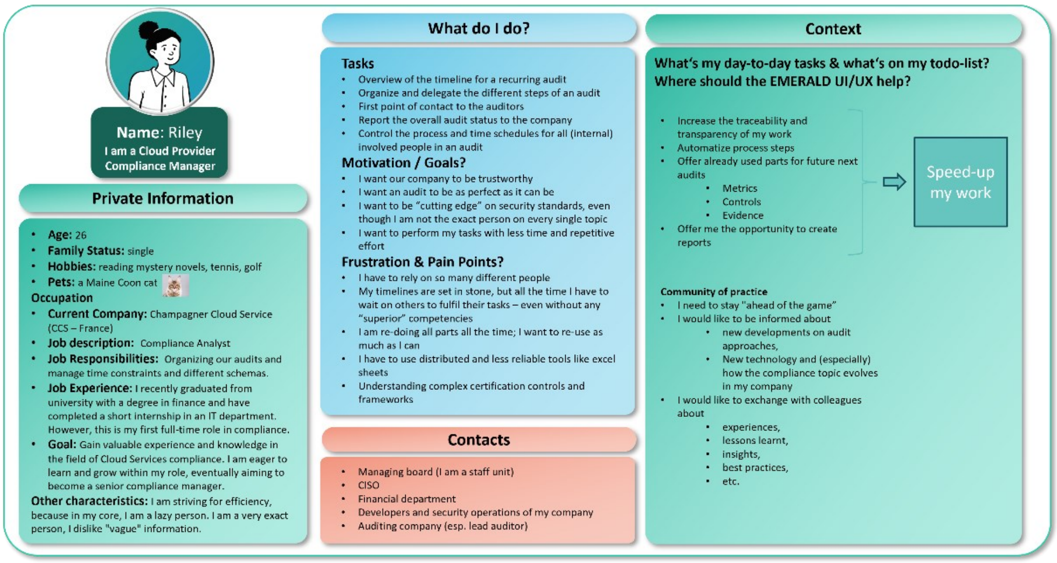

Compliance Stakeholders
" ... I want to be 'cutting edge' on security standards, even though I am not the exact person on every single topic ..."
Name: Riley
I am a Cloud Provider Compliance Manager
Name: Emerson
I am a Compliance Manager in Financial Service Institution.
Name: Dylan
I am an Internal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

Figure 29. Overview of the three stakeholder groups and the respective personas

5.1 Riley – Cloud Service Provider Compliance Manager

The first persona – a cloud service provider compliance manager – was named Riley and is depicted in Figure 30.

- **About Riley:** Riley is 26 years old, single, reads mystery novels, and has a Maine Coon cat as a pet. Riley recently graduated and has started the first full-time position as a compliance manager. Riley's responsibilities as a compliance analyst are organizing audits and managing the scheduling of different compliance schemes. Her/his overall goal is to gain experience as a compliance manager and grow to become a senior compliance manager.
- **Tasks, Motivation, and Pains:** Riley's tasks consist of checking audit timelines, organizing and delegating tasks during audits, being the contact person for auditors, and reporting audit status internally. Riley's goals are to support the company in being trustworthy, perfecting audit processes, being up to date with security standards, and performing tasks more efficiently. Pain points for Riley are the dependency on others to finish tasks timely, the lack of efficient audit tools, and the lack of understanding of complex certification frameworks.
- **Contacts:** Riley's contacts are the managing board of the company, the chief information security manager, the financial department, developers, and as external contacts, the auditing companies and auditors.
- **Work Context:** EMERALD should help Riley with the day-to-day tasks by speeding up the work. For that, traceability and transparency of the work should be ensured. Further, process steps should be automated, and metrics, controls and evidence should be made reusable for upcoming audits. Simplifying the creation of audit reports would also help Riley in their day-to-day work.



Name: Riley
I am a Cloud Provider Compliance Manager

Private Information

- **Age:** 26
- **Family Status:** single
- **Hobbies:** reading mystery novels, tennis, golf
- **Pets:** a Maine Coon cat

Occupation

- **Current Company:** Champagner Cloud Service (CCS – France)
- **Job description:** Compliance Analyst
- **Job Responsibilities:** Organizing our audits and manage time constraints and different schemas.
- **Job Experience:** I recently graduated from university with a degree in finance and have completed a short internship in an IT department. However, this is my first full-time role in compliance.
- **Goal:** Gain valuable experience and knowledge in the field of Cloud Services compliance. I am eager to learn and grow within my role, eventually aiming to become a senior compliance manager.

Other characteristics: I am striving for efficiency, because in my core, I am a lazy person. I am a very exact person, I dislike "vague" information.

What do I do?

Tasks

- Overview of the timeline for a recurring audit
- Organize and delegate the different steps of an audit
- First point of contact to the auditors
- Report the overall audit status to the company
- Control the process and time schedules for all (internal) involved people in an audit

Motivation / Goals?

- I want our company to be trustworthy
- I want an audit to be as perfect as it can be
- I want to be "cutting edge" on security standards, even though I am not the exact person on every single topic
- I want to perform my tasks with less time and repetitive effort

Frustration & Pain Points?

- I have to rely on so many different people
- My timelines are set in stone, but all the time I have to wait on others to fulfil their tasks – even without any "superior" competencies
- I am re-doing all parts all the time; I want to re-use as much as I can
- I have to use distributed and less reliable tools like excel sheets
- Understanding complex certification controls and frameworks

Contacts

- Managing board (I am a staff unit)
- CISO
- Financial department
- Developers and security operations of my company
- Auditing company (esp. lead auditor)

Context

What's my day-to-day tasks & what's on my todo-list? Where should the EMERALD UI/UX help?

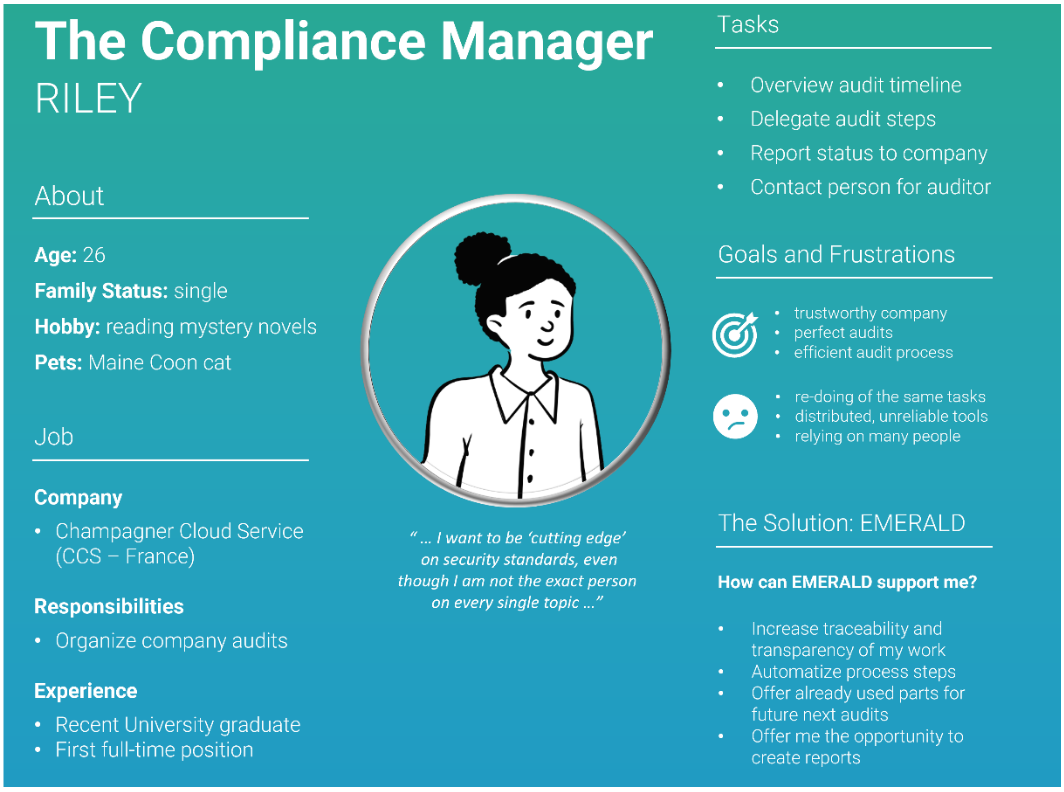
- Increase the traceability and transparency of my work
- Automatize process steps
- Offer already used parts for future next audits
  - Metrics
  - Controls
  - Evidence
- Offer me the opportunity to create reports

Community of practice

- I need to stay "ahead of the game"
- I would like to be informed about
  - new developments on audit approaches,
  - New technology and (especially) how the compliance topic evolves in my company
- I would like to exchange with colleagues about
  - experiences,
  - lessons learnt,
  - insights,
  - best practices,
  - etc.

Figure 30. Riley – Cloud Service Compliance Manager

Figure 31 summarizes Riley's main characteristic in a "persona-on-the-go".



The Compliance Manager

RILEY

About

Age: 26

Family Status: single

Hobby: reading mystery novels

Pets: Maine Coon cat

Job

Company

- Champagner Cloud Service (CCS – France)

Responsibilities

- Organize company audits

Experience

- Recent University graduate
- First full-time position

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

Tasks

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

Goals and Frustrations

- trustworthy company
- perfect audits
- efficient audit process

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

The Solution: EMERALD

How can EMERALD support me?

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

Figure 31. Persona-on-the-go for Riley – Cloud Service Compliance Manager

5.1.1 Scenario A: Riley – Managing a New Audit Scope

In this scenario, Riley's goal is to manage a new audit scope as shown in Figure 46 (in Section 10, *APPENDIX B*). From the C-Level Riley was informed that a new certification scheme for one of their cloud services needs to be used – namely BSI C5. Thus, they need to familiarize themselves with the new certification scheme and prepare the company for the new audit with the EMERALD solution. Therefore, Riley opens EMERALD and navigates to the *Certification Schemes* to upload a new certification scheme (EMERALD Components: *MARI*, *RCM*). Riley uses the *Control Mapping* function in EMERALD to find out which controls of the previously used EUCS do map to controls offered by the new scheme BSI C5, additionally the metrics of the corresponding controls in EUCS can be transferred. Riley also navigates to the *Metrics Mapping* to manually map metrics to controls. Then Riley sets up a target of evaluation which includes a three steps description of the cloud solution, setting up all relevant EMERALD extractors and enables, if desired, the *Trustworthiness System*. Riley creates an audit scope with the newly created target of evaluation and certification scheme and checks the respective assessment results and evidence of the controls retrieved so far. Lastly, Riley uses the newly created audit scope to manage the new certification scheme for the selected cloud service.

5.1.2 Scenario B: Riley – Manage all Controls of an Audit Scope

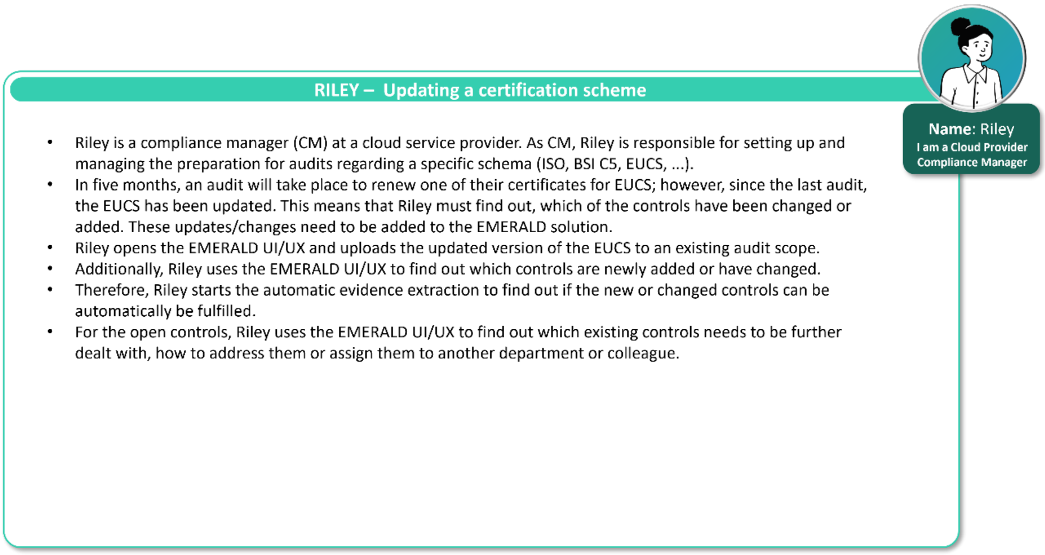
In this scenario, Riley is part of an audit that will take place in two months to renew certificates regarding EUCS as shown in Figure 47 (see Section 10, *APPENDIX B*). Riley checks the respective audit scope in the EMERALD UI to identify if all controls of the scheme can be met with some evidence (technical or organisational). Riley can use filters to better understand the overall status of the controls. Riley knows that all controls marked with a green checkmark are compliant. Riley can open the respective control (*Control Details View)* to get more information about the available assessment results. Additionally, Riley can either assign non-compliant controls directly to a person or department.

5.1.3 Scenario C: Riley – Uncover all "blind spots"

When preparing for an audit, Riley is responsible that all controls are fulfilled and there are no blind spots as shown in Figure 48 (see Section 10, *APPENDIX B*). In the EMERALD UI all controls have an owner (initial creator of the audit scope) and a status (compliant/ non-compliant). For further investigation Riley needs to distribute the non-compliant controls to a colleague or department by assigning them via the EMERALD UI to the respective control or metric. Any additional communication regarding a follow-up process and an escalation needs to be performed outside of EMERALD.

5.1.4 Scenario D: Riley – Updating a certification scheme

In this scenario, an audit will be conducted in five months to renew one of the certificates for EUCS. Since the last audit the EUCS has been updated, Riley needs to investigate which of the controls have been changed or added (this will not be supported by EMERALD). Riley opens the EMERALD UI and uploads the new EUCS version as a new certification scheme and creates a new audit scope. In the *Metrics Mapping* Riley can check for each control the associated metrics. In the respective *Audit Scope Overview* Riley discovers controls that are non-compliant and need to be further dealt with. For this process Riley uses the EMERALD UI to assign the non-compliant controls to another department or colleague. The scenario was revised from the original version by the pilot partners as presented in Figure 32 to transparently reflect that the initial description was not fully supported by the EMERALD UI, while ensuring the core use case remains viable.



RILEY – Updating a certification scheme

Name: Riley
I am a Cloud Provider Compliance Manager

- Riley is a compliance manager (CM) at a cloud service provider. As CM, Riley is responsible for setting up and managing the preparation for audits regarding a specific schema (ISO, BSI C5, EUCS, ...).
- In five months, an audit will take place to renew one of their certificates for EUCS; however, since the last audit, the EUCS has been updated. This means that Riley must find out, which of the controls have been changed or added. These updates/changes need to be added to the EMERALD solution.
- Riley opens the EMERALD UI/UX and uploads the updated version of the EUCS to an existing audit scope.
- Additionally, Riley uses the EMERALD UI/UX to find out which controls are newly added or have changed.
- Therefore, Riley starts the automatic evidence extraction to find out if the new or changed controls can be automatically be fulfilled.
- For the open controls, Riley uses the EMERALD UI/UX to find out which existing controls needs to be further dealt with, how to address them or assign them to another department or colleague.

Figure 32. Riley – Updating a certification scheme

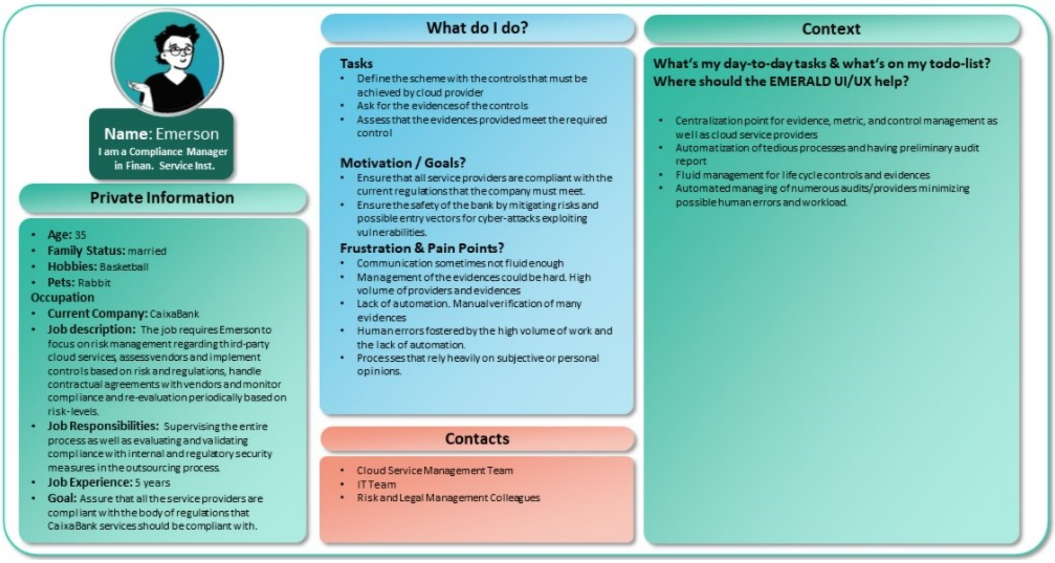
5.1.5 Scenario E: Riley – Accompanying an Audit

In this scenario, Riley is accompanying an audit. They are the most important contact person when an audit is taking place at the CSP as presented in Figure 49 (see Section 10, *APPENDIX B*). Riley is part of an audit team on the companies' site, to support the external auditors conducting the audit against a certain standard, e.g., EUCS or BSI C5 on the company's premises. The lead auditor has already selected a big sample of controls that need to be checked during the audit. To ensure that the cloud system is compliant with the selected controls, Riley can present the individual evidence of the controls in the EMERALD UI to the lead auditor.

5.2 Emerson - Compliance Manager in Financial Service Institution

The second persona – a compliance manager in a financial service institution – was named Emerson and is depicted in Figure 33.

- **About Emerson:** Emerson is 35 years old and married, plays basketball, and has a rabbit as a pet. Emerson has 5 years of experience in the current position. The job description states that Emerson focuses on risk management of third-party cloud services, assesses controls based on risk and regulation, manages contractual agreements, and monitors compliance. Responsibilities include process supervision, evaluating and validating compliance with security measures, and managing data privacy security. The overall goal of Emerson is to ensure that all service providers are compliant with given standards.
- **Tasks, Motivation and Pains:** Emerson's tasks consist of, among other things, the definition of the audit scheme including controls that must be fulfilled by the cloud service provider, and the assessment of provided evidence for respective controls. In that, goals are to ensure that all service providers comply with the current regulations and ensure safety by mitigating risks associated with audit requirements. Pain points in Emerson's day-to-day are that the communication with other departments is sometimes not fluid, tasks like verification of multiple evidence is not automated but must be done manually, and the management of a high volume of providers and their evidence is tough and time-consuming.
- **Contacts:** Emerson's workplace contacts are the cloud service management, IT, and legal teams.
- **Work Context:** EMERALD could help Emerson in the day-to-day tasks by providing a centralised point for evidence, metrics, and controls, further by automating tedious processes and management of numerous audits and thus minimizing human error and workload.



Name: Emerson
I am a Compliance Manager in Finan. Service Inst.

Private Information

- **Age:** 35
- **Family Status:** married
- **Hobbies:** Basketball
- **Pets:** Rabbit

Occupation

- **Current Company:** CaixaBank
- **Job description:** The job requires Emerson to focus on risk management regarding third-party cloud services, assess vendors and implement controls based on risk and regulations, handle contractual agreements with vendors and monitor compliance and re-evaluation periodically based on risk-levels.
- **Job Responsibilities:** Supervising the entire process as well as evaluating and validating compliance with internal and regulatory security measures in the outsourcing process.
- **Job Experience:** 5 years
- **Goal:** Assure that all the service providers are compliant with the body of regulations that CaixaBank services should be compliant with.

What do I do?

Tasks

- Define the scheme with the controls that must be achieved by cloud provider
- Ask for the evidences of the controls
- Assess that the evidences provided meet the required control

Motivation / Goals?

- Ensure that all service providers are compliant with the current regulations that the company must meet.
- Ensure the safety of the bank by mitigating risks and possible entry vectors for cyber-attacks exploiting vulnerabilities.

Frustration & Pain Points?

- Communication sometimes not fluid enough
- Management of the evidences could be hard. High volume of providers and evidences
- Lack of automation. Manual verification of many evidences
- Human errors fostered by the high volume of work and the lack of automation.
- Processes that rely heavily on subjective or personal opinions.

Contacts

- Cloud Service Management Team
- IT Team
- Risk and Legal Management Colleagues

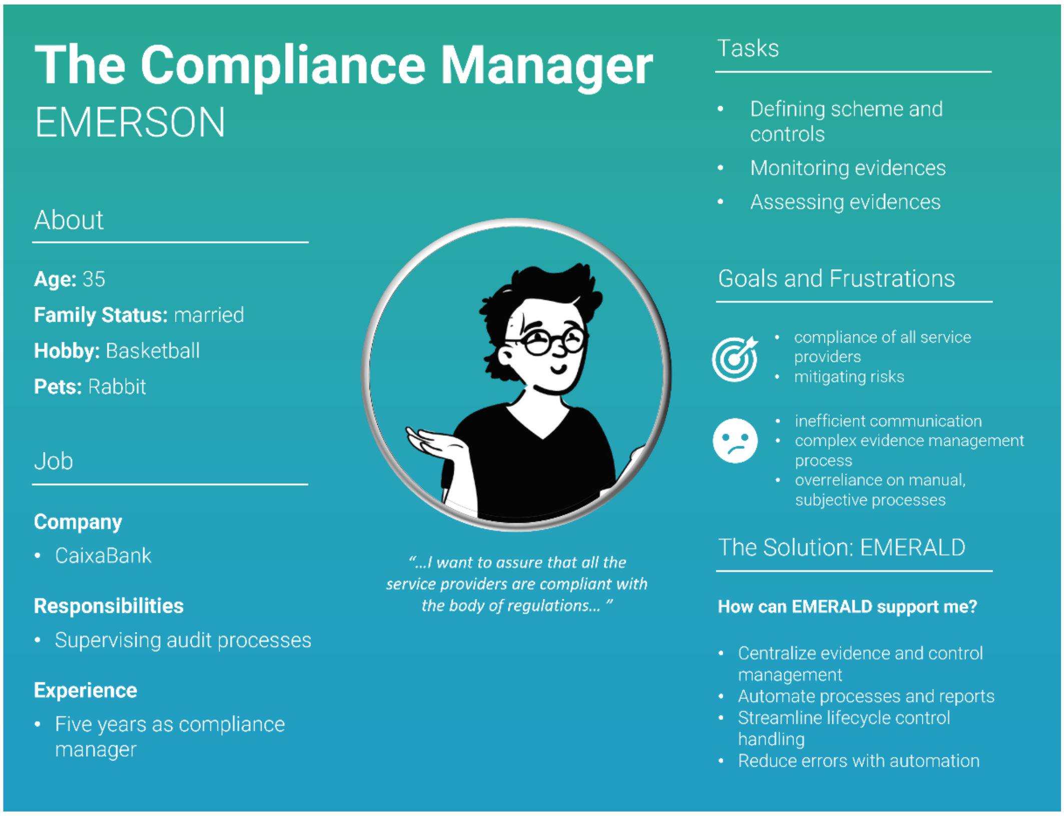
Context

What's my day-to-day tasks & what's on my todo-list? Where should the EMERALD UI/UX help?

- Centralization point for evidence, metric, and control management as well as cloud service providers
- Automatization of tedious processes and having preliminary audit report
- Fluid management for life cycle controls and evidences
- Automated managing of numerous audits/providers minimizing possible human errors and workload.

Figure 33. Emerson – Compliance Manager in Financial Service Institution

Figure 34 summarizes Emerson's main characteristic in a "persona-on-the-go".



The Compliance Manager

EMERSON

About

Age: 35
Family Status: married
Hobby: Basketball
Pets: Rabbit

Job

Company
- CaixaBank

Responsibilities
- Supervising audit processes

Experience
- Five years as compliance manager

"…I want to assure that all the service providers are compliant with the body of regulations… "

Tasks

- Defining scheme and controls
- Monitoring evidences
- Assessing evidences

Goals and Frustrations

- compliance of all service providers
- mitigating risks

- inefficient communication
- complex evidence management process
- overreliance on manual, subjective processes

The Solution: EMERALD

How can EMERALD support me?

- Centralize evidence and control management
- Automate processes and reports
- Streamline lifecycle control handling
- Reduce errors with automation

Figure 34. Persona-on-the-go for Emerson – Compliance Manager in financial services

5.2.1 Scenario: Emerson – Bring Your Own Certification Scheme

Generally, in this scenario Emerson's goal would be to define their own certification scheme, thus, the new certification scheme should be a selection and combination of controls from other certification schemes ("Bring Your Own Certification Scheme - BYOCS" option) as presented in Figure 50 (see Section 10 , *APPENDIX B*). Therefore, Emerson opens the view that allows to set up a new certification scheme and selects a set of controls from available certification schemes (e.g., EUCS, BSI C5). Their line manager then informs Emerson that Department X has decided to acquire a new cloud service provider - namely XYZ. Emerson creates an audit scope to manage cloud solutions and the corresponding BYOCS. Emerson opens EMERALD, selects the audit scope and the XYZ cloud solution to be audited, and uploads all relevant documents (links, etc.). Emerson's task is to go through and check all controls, for which Emerson goes to the EMERALD UI. Emerson uses different EMERALD UI functionalities to filter the controls and uses different visualizations of the overall status of all controls to determine which controls need to be dealt with and which are already compliant.

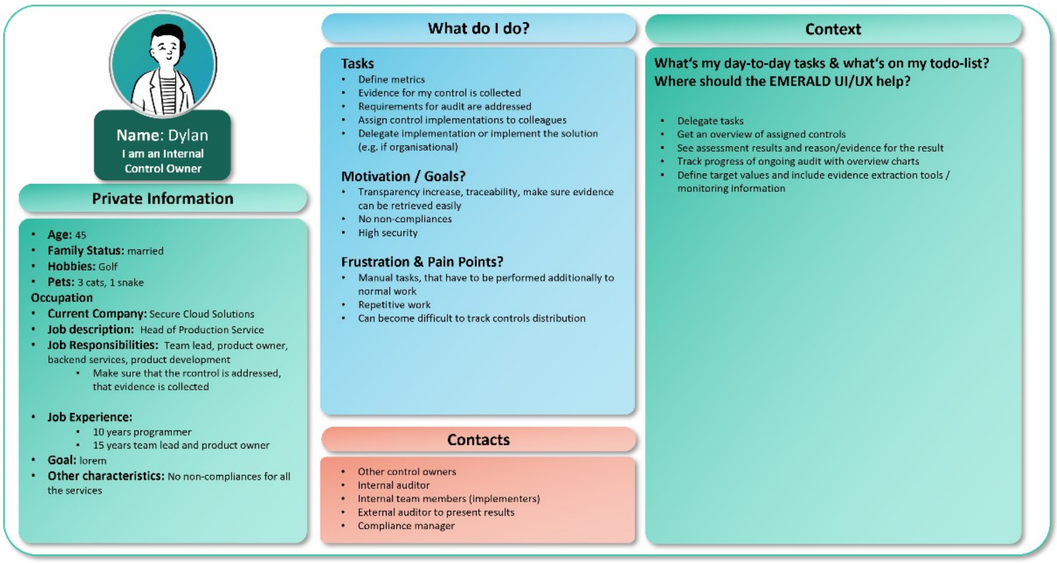
5.3 Dylan – Internal Control Owner

The third persona – an internal control owner – was named Dylan and is depicted in Figure 35.

- **About Dylan:** Dylan is 45 years old, married, enjoys golf and has three cats and one snake as pets. Dylan's job experience entails ten years as a programmer and fifteen years as a team lead and product owner. Dylan's responsibilities as head of production service include leading a team and overseeing and planning product development and backend services. Regarding audits, Dylan's responsibility is to ensure that controls are addressed, and all evidence is collected. The overall goal is to have no non-compliance for all services.
- **Tasks, Motivation and Pains:** Dylan's tasks consist of defining metrics, collecting evidence for controls, and assigning and delegating control implementation to the team. In that, the

goals are to increase transparency, traceability, and accessibility of evidence. Additional goals are to have no non-compliances and to ensure high security. Pain points are manual tasks that must be addressed in addition to the day-to-day activities, repetitive tasks, and tracking control distribution can be difficult.

- **Contacts:** Dylan's internal contacts in the company are other control owners, internal auditors, team members (especially implementers), and the compliance manager. Externally, Dylan gets in contact with auditors.
- **Work Context:** EMERALD could help Dylan in their day-to-day tasks by simply delegating tasks, providing an overview of assigned controls and displaying assessment results. Further, tracking the progress of ongoing audits and the possibility of defining target values and having evidence monitoring and extraction tools.



Name: Dylan
I am an Internal Control Owner

Private Information

- **Age:** 45
- **Family Status:** married
- **Hobbies:** Golf
- **Pets:** 3 cats, 1 snake

Occupation

- **Current Company:** Secure Cloud Solutions
- **Job description:** Head of Production Service
- **Job Responsibilities:** Team lead, product owner, backend services, product development
  - Make sure that the rcontrol is addressed, that evidence is collected
- **Job Experience:**
  - 10 years programmer
  - 15 years team lead and product owner
- **Goal:** lorem
- **Other characteristics:** No non-compliances for all the services

What do I do?

Tasks

- Define metrics
- Evidence for my control is collected
- Requirements for audit are addressed
- Assign control implementations to colleagues
- Delegate implementation or implement the solution (e.g. if organisational)

Motivation / Goals?

- Transparency increase, traceability, make sure evidence can be retrieved easily
- No non-compliances
- High security

Frustration & Pain Points?

- Manual tasks, that have to be performed additionally to normal work
- Repetitive work
- Can become difficult to track controls distribution

Contacts

- Other control owners
- Internal auditor
- Internal team members (implementers)
- External auditor to present results
- Compliance manager

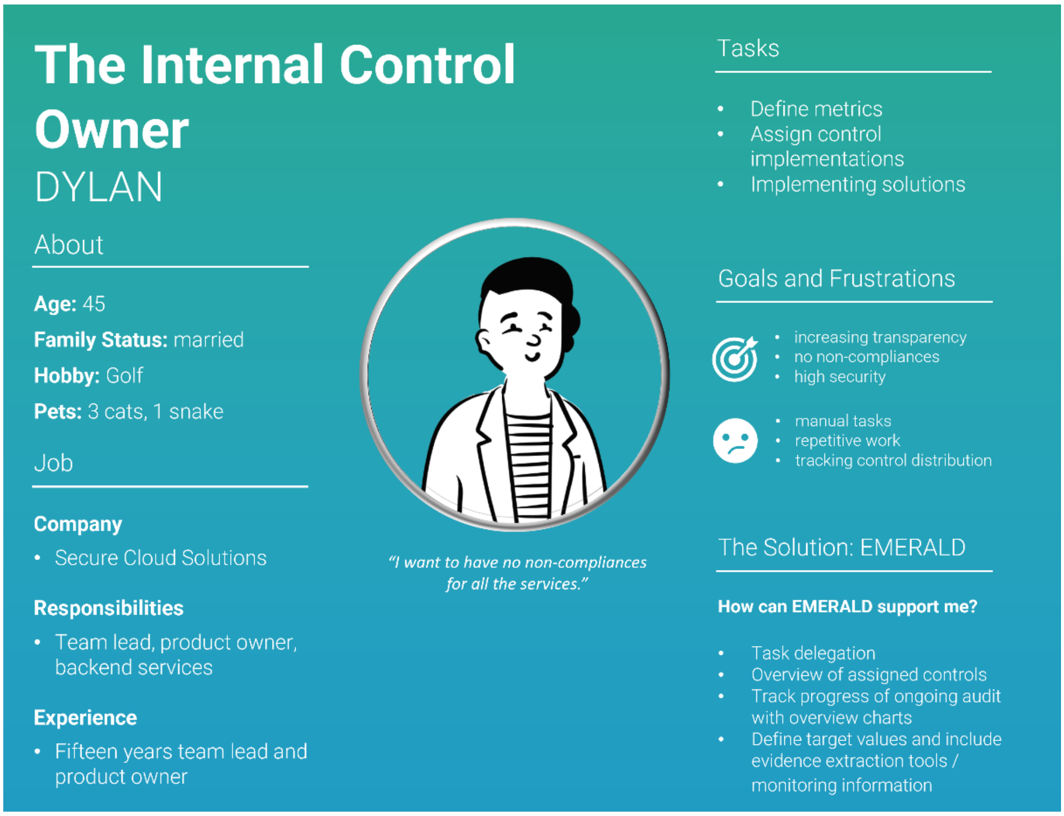
Context

What‘s my day-to-day tasks & what‘s on my todo-list? Where should the EMERALD UI/UX help?

- Delegate tasks
- Get an overview of assigned controls
- See assessment results and reason/evidence for the result
- Track progress of ongoing audit with overview charts
- Define target values and include evidence extraction tools / monitoring information

Figure 35. Dylan – Internal Control Owner

Figure 36 summarizes Dylan’s main characteristic in a “persona-on-the-go”.



The Internal Control Owner

DYLAN

About

Age: 45

Family Status: married

Hobby: Golf

Pets: 3 cats, 1 snake

Job

Company

- Secure Cloud Solutions

Responsibilities

- Team lead, product owner, backend services

Experience

- Fifteen years team lead and product owner

"I want to have no non-compliances for all the services."

Tasks

- Define metrics
- Assign control implementations
- Implementing solutions

Goals and Frustrations

- increasing transparency
- no non-compliances
- high security

- manual tasks
- repetitive work
- tracking control distribution

The Solution: EMERALD

How can EMERALD support me?

- Task delegation
- Overview of assigned controls
- Track progress of ongoing audit with overview charts
- Define target values and include evidence extraction tools / monitoring information

Figure 36. Persona-on-the-go for Dylan – Internal Control Owner

5.3.1 Scenario: Dylan – Internal Control Owner Control Implementation

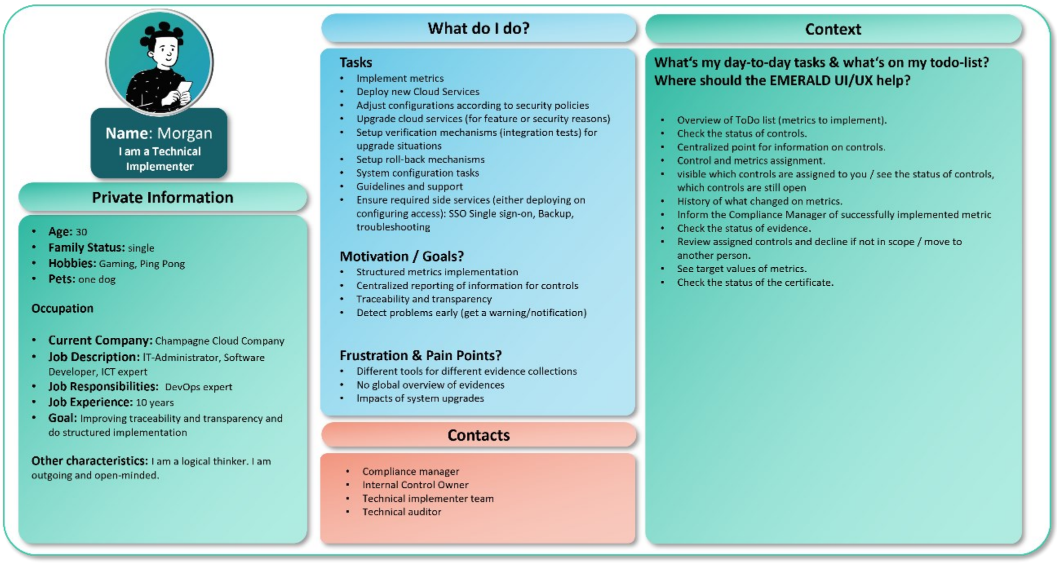
Overall, in this scenario Dylan opens the EMERALD UI, assesses a control that is still open and would like to delegate the implementation of this control to a colleague Y as presented in Figure 51 (see Section 10 , *APPENDIX B*). Y selects a set of metrics that matches the controls, implements the control and informs Dylan via the EMERALD UI that the metric was implemented. Dylan checks whether the metric has been implemented correctly and meets the control.

5.4 Morgan – Technical Implementer

The fourth persona – a technical implementer (metric implementer, developers, etc.) – was named Morgan and is depicted in Figure 37.

- **About Morgan:** Morgan is 30 years old, single, a dog owner and enjoys gaming and ping pong. Morgan has been working in DevOps for ten years and their current responsibilities are as a DevOps Expert. Morgan's overall goal is to improve traceability and transparency as well as to have a more structured approach to implementation.
- **Tasks, Motivation and Pains:** Morgan's tasks, among others, include implementing metrics, deploying new cloud services, adjusting configurations to align with security policies, and setting up verification mechanisms for upgrades. Ensuring a structured approach to metric implementation, centralized reporting, and clear visibility into controls is crucial. Morgan's focus is on early problem detection, maintaining traceability and ensuring transparency across all processes. Pain points include diverse tools for the evidence collectors, no overview of evidence, and impacts of system upgrades.
- **Contacts:** Morgan is solely communicating internally with the compliance manager, internal control owner and technical implementer as well as a technical auditor.

- **Work Context:** In Morgan’s daily activities, the EMERALD UI could enhance the workflow by offering a comprehensive to-do list, allowing Morgan to easily track which controls are assigned to them. It could also display an overview of metrics, including values, history, and status, with the ability to directly notify the compliance manager when a metric is successfully implemented. A central information hub would provide quick access to control statuses and would enable Morgan to review and reassess assigned controls, with the option to decline those out of scope. Additionally, the EMERALD UI could allow Morgan to check the status of certificates and evidence, ensuring all relevant information is easily accessible in one place.



Name: Morgan
I am a Technical Implementer

Private Information

- **Age:** 30
- **Family Status:** single
- **Hobbies:** Gaming, Ping Pong
- **Pets:** one dog

Occupation

- **Current Company:** Champagne Cloud Company
- **Job Description:** IT-Administrator, Software Developer, ICT expert
- **Job Responsibilities:** DevOps expert
- **Job Experience:** 10 years
- **Goal:** Improving traceability and transparency and do structured implementation

Other characteristics: I am a logical thinker. I am outgoing and open-minded.

What do I do?

Tasks

- Implement metrics
- Deploy new Cloud Services
- Adjust configurations according to security policies
- Upgrade cloud services (for feature or security reasons)
- Setup verification mechanisms (integration tests) for upgrade situations
- Setup roll-back mechanisms
- System configuration tasks
- Guidelines and support
- Ensure required side services (either deploying on configuring access): SSO Single sign-on, Backup, troubleshooting

Motivation / Goals?

- Structured metrics implementation
- Centralized reporting of information for controls
- Traceability and transparency
- Detect problems early (get a warning/notification)

Frustration & Pain Points?

- Different tools for different evidence collections
- No global overview of evidences
- Impacts of system upgrades

Contacts

- Compliance manager
- Internal Control Owner
- Technical implementer team
- Technical auditor

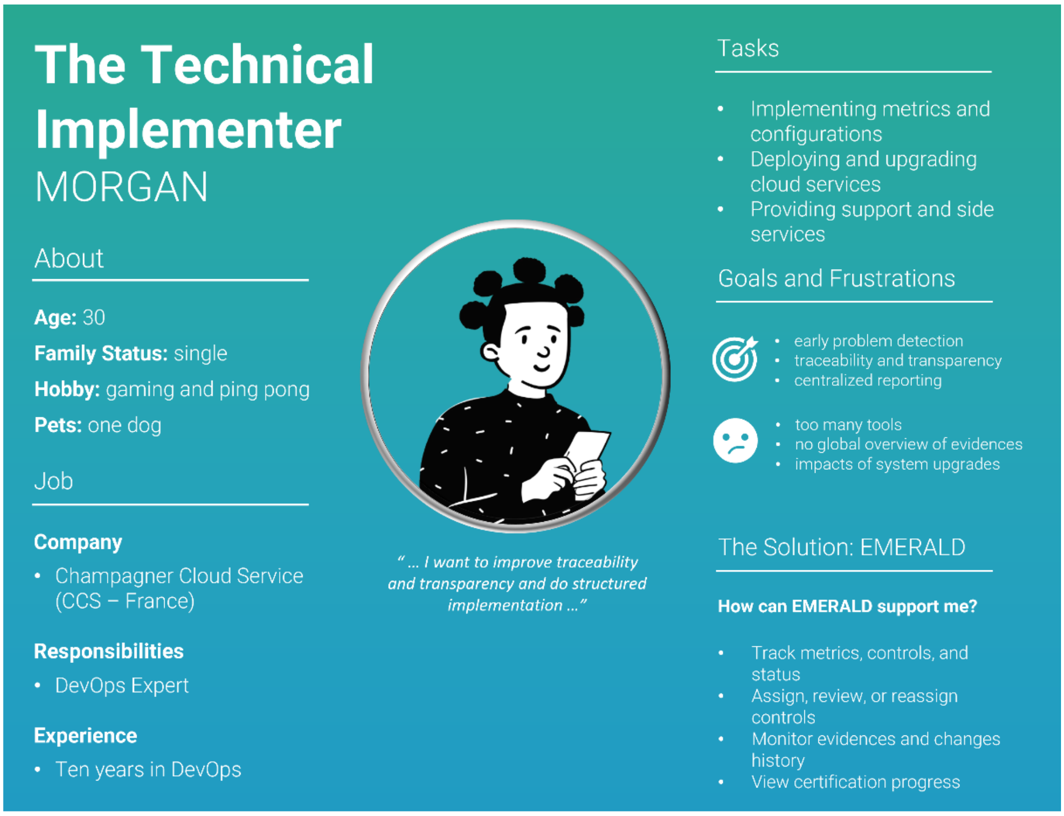
Context

What‘s my day-to-day tasks & what‘s on my todo-list? Where should the EMERALD UI/UX help?

- Overview of ToDo list (metrics to implement).
- Check the status of controls.
- Centralized point for information on controls.
- Control and metrics assignment.
- visible which controls are assigned to you / see the status of controls, which controls are still open
- History of what changed on metrics.
- Inform the Compliance Manager of successfully implemented metric
- Check the status of evidence.
- Review assigned controls and decline if not in scope / move to another person.
- See target values of metrics.
- Check the status of the certificate.

Figure 37. Morgan – Technical Implementer

Figure 38 summarizes Morgan’s main characteristic in a “persona-on-the-go”.



The Technical Implementer
MORGAN

About

Age: 30
Family Status: single
Hobby: gaming and ping pong
Pets: one dog

Job

Company
- Champagner Cloud Service (CCS – France)

Responsibilities
- DevOps Expert

Experience
- Ten years in DevOps

"… I want to improve traceability and transparency and do structured implementation …"

Tasks

- Implementing metrics and configurations
- Deploying and upgrading cloud services
- Providing support and side services

Goals and Frustrations

- early problem detection
- traceability and transparency
- centralized reporting

- too many tools
- no global overview of evidences
- impacts of system upgrades

The Solution: EMERALD

How can EMERALD support me?

- Track metrics, controls, and status
- Assign, review, or reassign controls
- Monitor evidences and changes history
- View certification progress

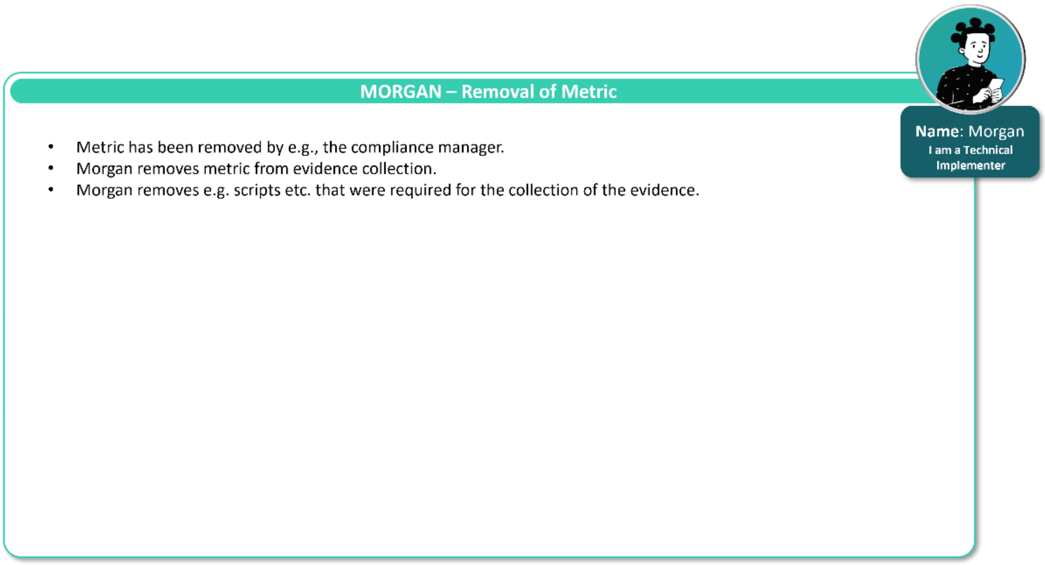
Figure 38. Persona-on-the-go for Morgan – Technical Implementer

5.4.1 Scenario A: Morgan – Checking Metrics and Evidence

In this scenario, Morgan is checking their assigned metrics as presented in Figure 52 (see Section 10 , *APPENDIX B*). They begin by selecting an evidence extraction tool and verifying the accuracy of the target values for the specific metric. Additionally, they review the status of the evidence and controls associated with previously processed metrics. If everything is correct, Morgan notifies the compliance manager that the metrics have been successfully implemented. If issues arise, they return to the specific metrics to troubleshoot and debug.

5.4.2 Scenario B: Morgan – Removal of Metric

In this scenario, Morgan previously had to manually remove metrics and related scripts. With the EMERALD UI, manual removal of metrics is no longer necessary, though the underlying use case remains valid. Instead, EMERALD offers the *Metrics Mapping* function where metrics can be assigned and unassigned to a specific control. Due to this direct support in the EMERALD UI, compliance managers can now directly make these changes themselves when doing the mapping of metrics to controls. Thus, there is no need for Morgan to remove or adapt anything. For transparency and completeness, the scenario is still presented in its original form in Figure 39.



MORGAN – Removal of Metric

- Metric has been removed by e.g., the compliance manager.
- Morgan removes metric from evidence collection.
- Morgan removes e.g. scripts etc. that were required for the collection of the evidence.

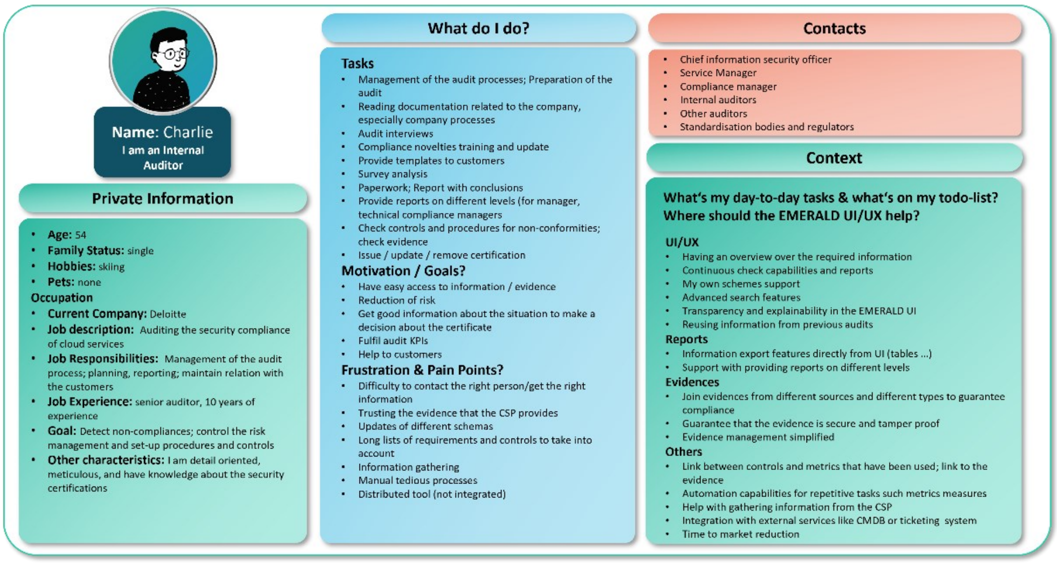
Name: Morgan
I am a Technical Implementer

Figure 39. Scenario B: Morgan – Removal of Metric

5.5 Charlie – Internal Auditor

The fifth persona – an internal auditor – was named Charlie and is depicted in Figure 40.

- **About Charlie:** Charlie is a senior auditor with ten years of job experience. Charlie is detail-oriented and meticulous and has knowledge of security certifications. As an auditor for security compliance with cloud services, Charlie's responsibilities include managing the audit process, planning, reporting, and maintaining contact with customers. The overall goal is to detect non-compliances, control risk management, and set up procedures. Charlie did not want to provide any further personal information.
- **Tasks, Motivation and Pains:** Charlie's tasks include managing audit processes, preparing audits, conducting audit interviews, and participating in compliance novelties training. Further, Charlie provides templates to customers, surveys analysis, reports on different levels (organizational, technical), checks controls and procedures for non-conformities and evidence. In that, the goals are to provide easy access to information/evidence, reduce risks, fulfil audit KPIs, and help customers. Pain points are to get in contact with the responsible person and get the correct information, update different schemes, consider a vast number of requirements and controls for audits, manual, tedious processes, and distributed tools used during the audit.
- **Contacts:** Charlie is in contact with chief information security officers, service managers, compliance managers, other auditors, and standardization bodies and regulators.
- **Work Context:** In Charlie's day-to-day activities, the EMERALD UI could help by providing an overview of the required information, enabling continuous checks of capabilities and reports, making their own schemes integrable, enabling advanced search features, and making information from previous audits reusable. Regarding reporting, Charlie could be supported by providing information export features in the EMERALD UI and for example generating reports on different levels of detail. Regarding evidence, Charlie would need access to a simplified evidence management system where it is possible to join evidence from different sources. Additionally, EMERALD could help Charlie by automating repetitive tasks, such as measuring metrics, enabling information exchange with cloud service providers, and integrating external services, e.g., ticketing systems.



Name: Charlie
I am an Internal Auditor

Private Information

- **Age:** 54
- **Family Status:** single
- **Hobbies:** skiing
- **Pets:** none

Occupation

- **Current Company:** Deloitte
- **Job description:** Auditing the security compliance of cloud services
- **Job Responsibilities:** Management of the audit process; planning, reporting; maintain relation with the customers
- **Job Experience:** senior auditor, 10 years of experience
- **Goal:** Detect non-compliances; control the risk management and set-up procedures and controls
- **Other characteristics:** I am detail oriented, meticulous, and have knowledge about the security certifications

What do I do?

Tasks

- Management of the audit processes; Preparation of the audit
- Reading documentation related to the company, especially company processes
- Audit interviews
- Compliance novelties training and update
- Provide templates to customers
- Survey analysis
- Paperwork; Report with conclusions
- Provide reports on different levels (for manager, technical compliance managers
- Check controls and procedures for non-conformities; check evidence
- Issue / update / remove certification

Motivation / Goals?

- Have easy access to information / evidence
- Reduction of risk
- Get good information about the situation to make a decision about the certificate
- Fulfil audit KPIs
- Help to customers

Frustration & Pain Points?

- Difficulty to contact the right person/get the right information
- Trusting the evidence that the CSP provides
- Updates of different schemas
- Long lists of requirements and controls to take into account
- Information gathering
- Manual tedious processes
- Distributed tool (not integrated)

Contacts

- Chief information security officer
- Service Manager
- Compliance manager
- Internal auditors
- Other auditors
- Standardisation bodies and regulators

Context

What‘s my day-to-day tasks & what‘s on my todo-list? Where should the EMERALD UI/UX help?

UI/UX

- Having an overview over the required information
- Continuous check capabilities and reports
- My own schemes support
- Advanced search features
- Transparency and explainability in the EMERALD UI
- Reusing information from previous audits

Reports

- Information export features directly from UI (tables …)
- Support with providing reports on different levels

Evidences

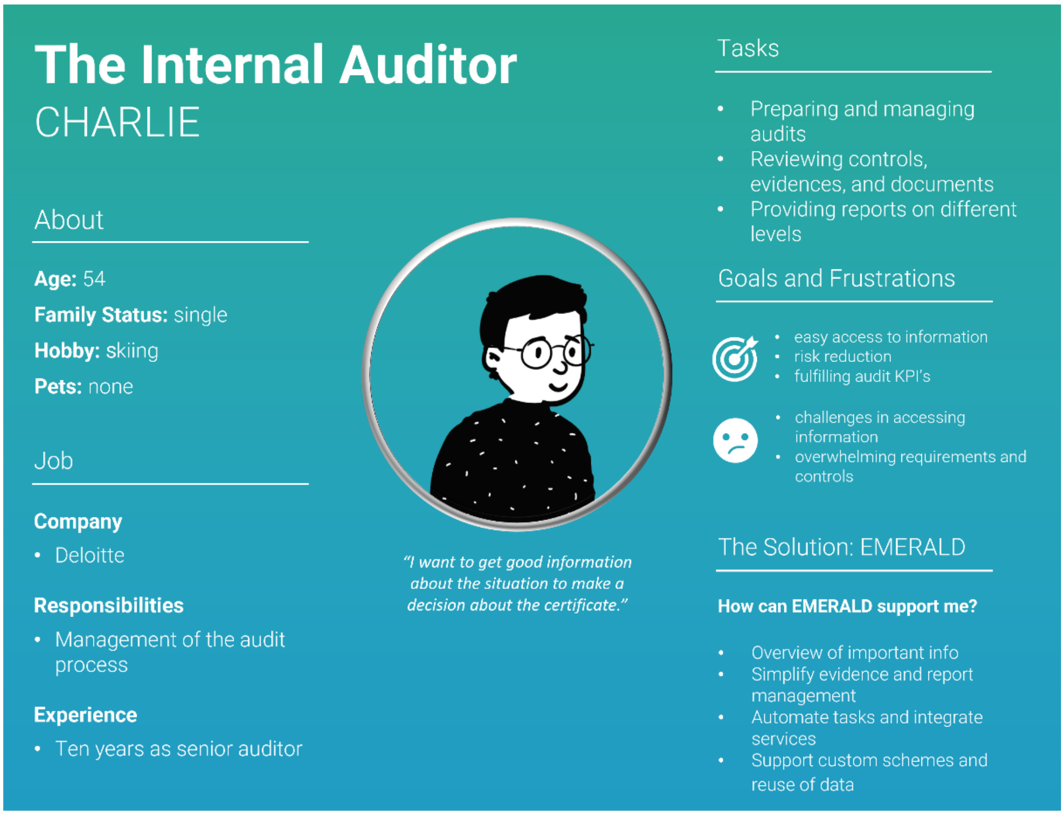
- Join evidences from different sources and different types to guarantee compliance
- Guarantee that the evidence is secure and tamper proof
- Evidence management simplified

Others

- Link between controls and metrics that have been used; link to the evidence
- Automation capabilities for repetitive tasks such metrics measures
- Help with gathering information from the CSP
- Integration with external services like CMDB or ticketing system
- Time to market reduction

Figure 40. Charlie – Auditor

Figure 41 summarizes Charlie's main characteristic in a "persona-on-the-go".



The Internal Auditor
CHARLIE

About

Age: 54
Family Status: single
Hobby: skiing
Pets: none

Job

Company

- Deloitte

Responsibilities

- Management of the audit process

Experience

- Ten years as senior auditor

"I want to get good information about the situation to make a decision about the certificate."

Tasks

- Preparing and managing audits
- Reviewing controls, evidences, and documents
- Providing reports on different levels

Goals and Frustrations

- easy access to information
- risk reduction
- fulfilling audit KPI's

- challenges in accessing information
- overwhelming requirements and controls

The Solution: EMERALD

How can EMERALD support me?

- Overview of important info
- Simplify evidence and report management
- Automate tasks and integrate services
- Support custom schemes and reuse of data

Figure 41. Persona-on-the-go: Charlie – Internal Auditor

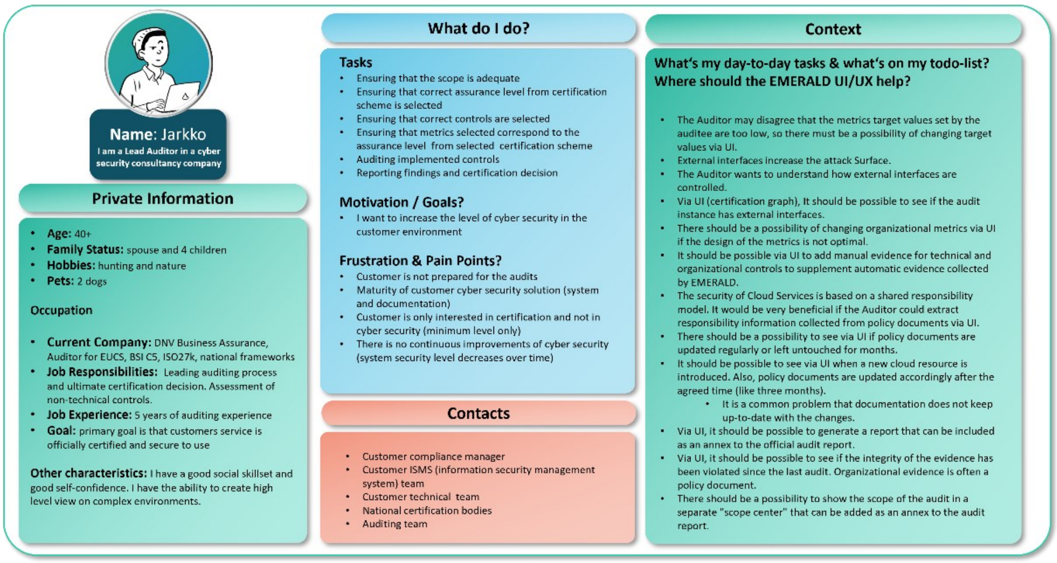
5.5.1 Scenario: Charlie – Preparation of an Audit by an Internal Auditor

Charlie would like to review all controls according to their compliance status in this scenario as presented in Figure 53 (see Section 10 , *APPENDIX B*). Charlie enters the EMERALD UI, looks for the controls related to EUCS high and looks for controls which are marked as non-compliant. Charlie has a closer look at the reasons of non-compliance; thus, it should be clear which metric/assessment result is causing the non-compliance so that the compliance manager can be informed. Once Charlie has reviewed all non-compliances, an internal report should be created for the compliance manager.

5.6 Jarkko – Lead Auditor

The sixth persona – an auditor – was named Jarkko and is depicted in Figure 42.

- **About Jarkko:** Jarkko is over 40 years old, married and has four kids. They love to hunt and be in nature with their two dogs. Jarkko is a lead auditor in a cyber security consultancy company with five years of auditing experience. Leading the auditing process and ultimate certification decision, as well as assessment of non-technical requirements are their job responsibilities. Jarkko's primary goal is that customer services are officially certified and secure.
- **Tasks, Motivation and Pains:** Jarkko needs to ensure that the scope is adequate, the correct assurance level from the certification scheme and controls are selected, and the metrics selected corresponds to the assurance level from the selected certification scheme. Further, Jarkko checks during the audit whether the respective controls are implemented and reports findings and certification decisions. Their motivation is to increase cyber security in the customer environment. Pain points mentioned are that the customer is not prepared for the audits, the maturity and non-continuous improvement of the customer's cyber security and that the customer is only interested in getting the certification and not in cybersecurity.
- **Contacts:** Jarkko is in contact with the customer compliance manager, customer information security management team, customer technical team, national certification bodies and auditing team.
- **Work Context:** In Jarkko's day-to-day activities, the EMERALD UI could improve the auditor's flexibility to modify target metrics values if they are set too low. An overview of external interfaces helps to ensure that there are no unnecessary external interfaces that increase the attack surface and provides information on how external interfaces are controlled. The EMERALD UI should support Jarkko by providing the possibility to change organizational metrics and add manual evidence for technical and organizational controls to supplement automatic evidence by EMERALD (this will not be provided in EMERALD – auditors will only have read access to the controls and the mapped metrics). Regarding policy documents there should be an overview to see if the policy documents are updated regularly (after agreed time) and the ability for the auditor to extract responsibilities from the policy documents. Additionally, it should be possible for Jarkko to see if a new cloud resource is introduced. The EMERALD UI should support the creation of the annex of the official audit report by generating a report and show the scope of the audit in a separate "scope center" which can also be added as an annex to the audit report. Further it should be possible for Jarkko to see if the integrity of the evidence has been violated since the last audit.



Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company

Private Information

- **Age:** 40+
- **Family Status:** spouse and 4 children
- **Hobbies:** hunting and nature
- **Pets:** 2 dogs

Occupation

- **Current Company:** DNV Business Assurance, Auditor for EUCS, BSI C5, ISO27k, national frameworks
- **Job Responsibilities:** Leading auditing process and ultimate certification decision. Assessment of non-technical controls.
- **Job Experience:** 5 years of auditing experience
- **Goal:** primary goal is that customers service is officially certified and secure to use

Other characteristics: I have a good social skillset and good self-confidence. I have the ability to create high level view on complex environments.

What do I do?

Tasks

- Ensuring that the scope is adequate
- Ensuring that correct assurance level from certification scheme is selected
- Ensuring that correct controls are selected
- Ensuring that metrics selected correspond to the assurance level from selected certification scheme
- Auditing implemented controls
- Reporting findings and certification decision

Motivation / Goals?

- I want to increase the level of cyber security in the customer environment

Frustration & Pain Points?

- Customer is not prepared for the audits
- Maturity of customer cyber security solution (system and documentation)
- Customer is only interested in certification and not in cyber security (minimum level only)
- There is no continuous improvements of cyber security (system security level decreases over time)

Contacts

- Customer compliance manager
- Customer ISMS (information security management system) team
- Customer technical team
- National certification bodies
- Auditing team

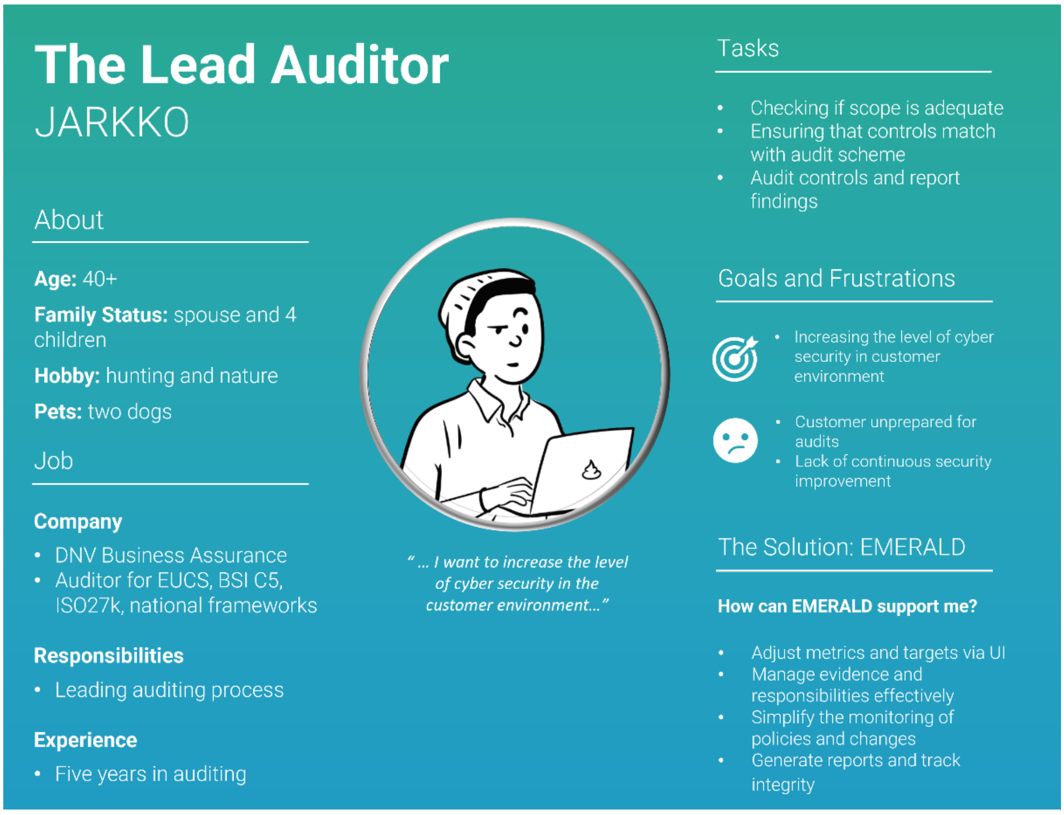
Context

What‘s my day-to-day tasks & what‘s on my todo-list? Where should the EMERALD UI/UX help?

- The Auditor may disagree that the metrics target values set by the auditee are too low, so there must be a possibility of changing target values via UI.
- External interfaces increase the attack Surface.
- The Auditor wants to understand how external interfaces are controlled.
- Via UI (certification graph), It should be possible to see if the audit instance has external interfaces.
- There should be a possibility of changing organizational metrics via UI if the design of the metrics is not optimal.
- It should be possible via UI to add manual evidence for technical and organizational controls to supplement automatic evidence collected by EMERALD.
- The security of Cloud Services is based on a shared responsibility model. It would be very beneficial if the Auditor could extract responsibility information collected from policy documents via UI.
- There should be a possibility to see via UI if policy documents are updated regularly or left untouched for months.
- It should be possible to see via UI when a new cloud resource is introduced. Also, policy documents are updated accordingly after the agreed time (like three months).
    - It is a common problem that documentation does not keep up-to-date with the changes.
- Via UI, it should be possible to generate a report that can be included as an annex to the official audit report.
- Via UI, it should be possible to see if the integrity of the evidence has been violated since the last audit. Organizational evidence is often a policy document.
- There should be a possibility to show the scope of the audit in a separate "scope center" that can be added as an annex to the audit report.

Figure 42. Jarkko – Lead Auditor

Figure 43 summarizes Jarkko's main characteristic in a "persona-on-the-go".



The Lead Auditor
JARKKO

About

Age: 40+

Family Status: spouse and 4 children

Hobby: hunting and nature

Pets: two dogs

Job

Company

- DNV Business Assurance
- Auditor for EUCS, BSI C5, ISO27k, national frameworks

Responsibilities

- Leading auditing process

Experience

- Five years in auditing

" … I want to increase the level of cyber security in the customer environment…"

Tasks

- Checking if scope is adequate
- Ensuring that controls match with audit scheme
- Audit controls and report findings

Goals and Frustrations

- Increasing the level of cyber security in customer environment

- Customer unprepared for audits
- Lack of continuous security improvement

The Solution: EMERALD

How can EMERALD support me?

- Adjust metrics and targets via UI
- Manage evidence and responsibilities effectively
- Simplify the monitoring of policies and changes
- Generate reports and track integrity

Figure 43. Persona-on-the-go for Jarkko – Lead Auditor

5.6.1 Scenario A: Jarkko – Scoping

Jarkko works for an external auditing company NIXU/DNV and they have been selected to perform auditing for a new cloud service to officially certify it as presented in Figure 54 (see Section 10, *APPENDIX B*). Jarkko and a technical auditor review the organizational and technical controls to prepare for the audit. In the EMERALD UI, Jarkko and his colleague can get an overview of the audit scope.

5.6.2 Scenario B: Jarkko – Preparing for Audit

To prepare for the audit, Jarkko needs to have access to the relevant EMERALD project and to the information about the validity/trustworthiness/applicability of the tools used for the audit as presented in see Figure 55 (see Section 10, *APPENDIX B*). They need to review the scope of the audit and be able to check metrics and target values. If the EUCS is used, Jarkko also needs to be able to review the self-assessment questionnaire. Further, they need to review the corresponding documentation.

5.6.3 Scenario C: Jarkko – Organizational Audit

In the organizational audit, Jarkko checks the integrity and compliance status of the controls and the corresponding assessment results and the regularity in which the policy documents are updated as presented in Figure 56 (see Section 10, *APPENDIX B*). They trust the EMERALD solution; therefore, they merely check the results of the controls that are not fulfilled (not compliant, no result). Jarkko is in communication with the compliance manager and if necessary, technical implementers. Lastly Jarkko adds the outcomes of his review to the audit report.

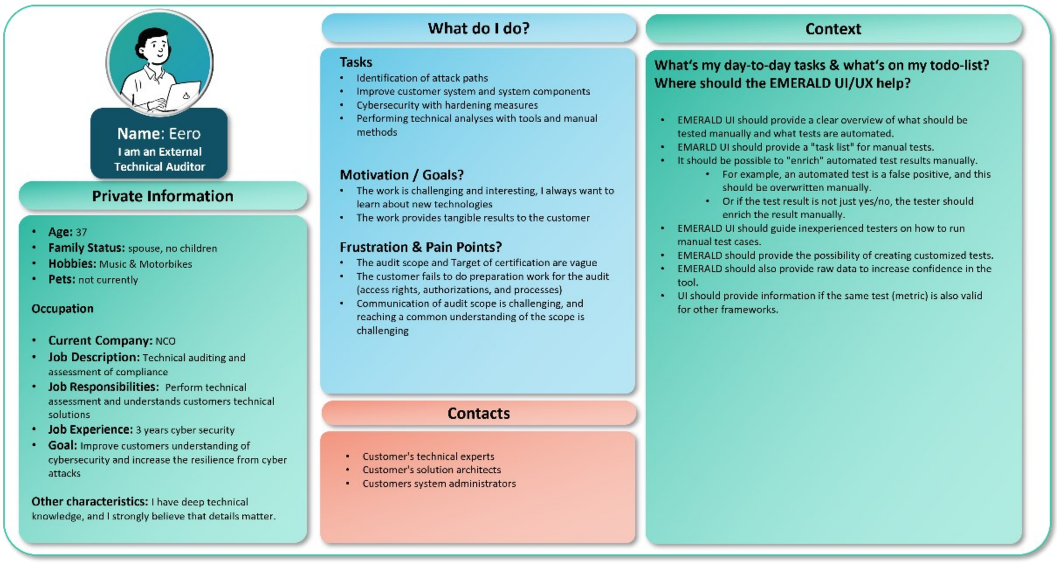
5.6.4 Scenario D: Jarkko – Certification

For the certification scenario, Jarkko needs to create an audit report and translates all non-compliances into reports as presented in Figure 57 (see Section 10, *APPENDIX B*). Jarkko communicates the findings and can create a report of the audit scope in the EMERALD UI that can be added to the audit report.

5.7 Eero – Technical Auditor

The seventh persona – technical auditor – was named Eero and is depicted in Figure 44.

- **About Eero:** Eero is 37 years old, married, enjoys music and motorbikes. Eero has three years of experience in cyber security and currently works as a technical auditor for external companies. Eero’s responsibilities include performing technical assessments and understanding the customers technical solutions. The overall goals are to improve customer’s understanding of cybersecurity and increase the resilience of cyberattacks.
- **Tasks, Motivation and Pains:** Eero’s tasks consist of identifying the attack paths, improving the customer system, system components and cybersecurity by hardening measures. Eero also performs technical analysis using tools and manual methods. Eero’s motivation is to provide tangible results to the customer. Pain Points are if the audit scope and target of certification are vague, the customer fails to prepare for the audit and fails to align on a common understanding of the scope.
- **Contacts:** Eero’s contacts are customers’ technical experts, solution architects and system administrators.
- **Work Context:** In Eero's day-to-day activities, the EMERALD UI could improve the overview of testing by including an overview of what should be tested manually (“task list”) and what was tested automatically. The automated test results should be adaptable to be manually enriched (this will not be implemented in EMERALD) and provide raw data to increase confidence in EMERALD. Additionally, Eero would like the possibility to create customized tests and receive information if the same test (metric) is also valid for other framework(s).



Name: Eero
I am an External Technical Auditor

Private Information

- **Age:** 37
- **Family Status:** spouse, no children
- **Hobbies:** Music & Motorbikes
- **Pets:** not currently

Occupation

- **Current Company:** NCO
- **Job Description:** Technical auditing and assessment of compliance
- **Job Responsibilities:** Perform technical assessment and understands customers technical solutions
- **Job Experience:** 3 years cyber security
- **Goal:** Improve customers understanding of cybersecurity and increase the resilience from cyber attacks

Other characteristics: I have deep technical knowledge, and I strongly believe that details matter.

What do I do?

Tasks

- Identification of attack paths
- Improve customer system and system components
- Cybersecurity with hardening measures
- Performing technical analyses with tools and manual methods

Motivation / Goals?

- The work is challenging and interesting, I always want to learn about new technologies
- The work provides tangible results to the customer

Frustration & Pain Points?

- The audit scope and Target of certification are vague
- The customer fails to do preparation work for the audit (access rights, authorizations, and processes)
- Communication of audit scope is challenging, and reaching a common understanding of the scope is challenging

Contacts

- Customer's technical experts
- Customer's solution architects
- Customers system administrators

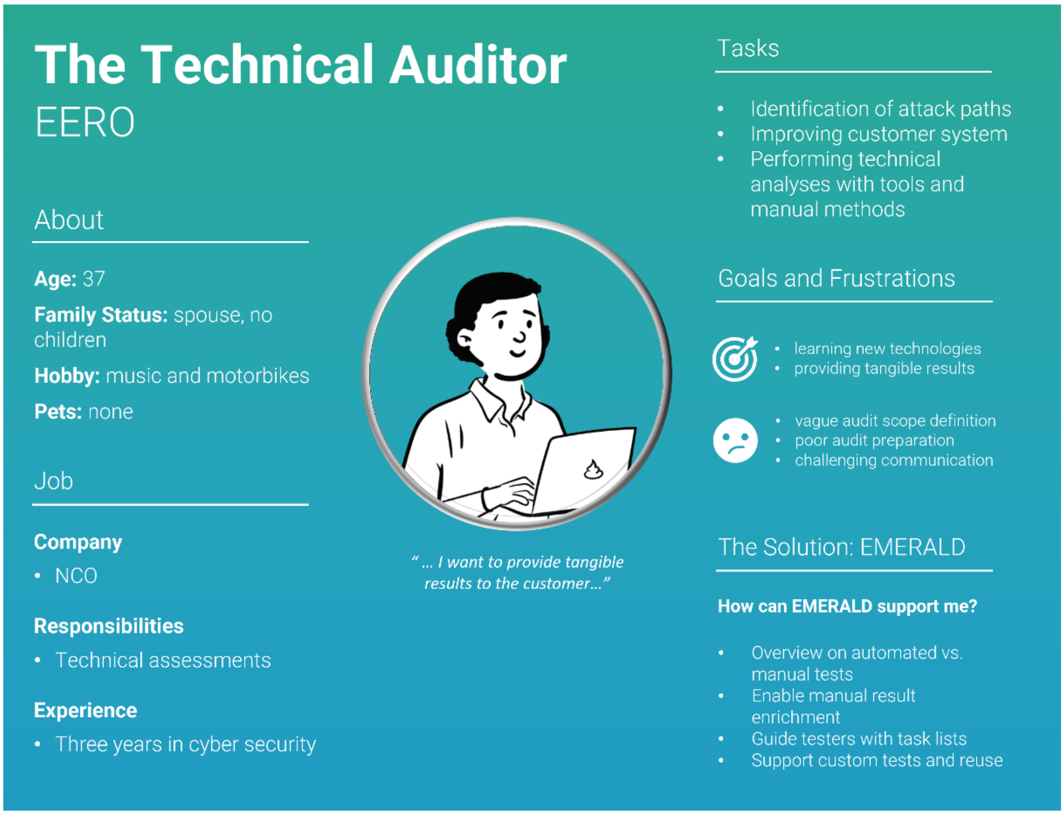
Context

What‘s my day-to-day tasks & what‘s on my todo-list? Where should the EMERALD UI/UX help?

- EMERALD UI should provide a clear overview of what should be tested manually and what tests are automated.
- EMARLD UI should provide a "task list" for manual tests.
- It should be possible to "enrich" automated test results manually.
  - For example, an automated test is a false positive, and this should be overwritten manually.
  - Or if the test result is not just yes/no, the tester should enrich the result manually.
- EMERALD UI should guide inexperienced testers on how to run manual test cases.
- EMERALD should provide the possibility of creating customized tests.
- EMERALD should also provide raw data to increase confidence in the tool.
- UI should provide information if the same test (metric) is also valid for other frameworks.

Figure 44. Eero – Technical Auditor

Figure 45 summarizes Eero’s main characteristic in a “persona-on-the-go”.



The Technical Auditor
EERO

About

Age: 37

Family Status: spouse, no children

Hobby: music and motorbikes

Pets: none

Job

Company
- NCO

Responsibilities
- Technical assessments

Experience
- Three years in cyber security

“ … I want to provide tangible results to the customer…”

Tasks

- Identification of attack paths
- Improving customer system
- Performing technical analyses with tools and manual methods

Goals and Frustrations

- learning new technologies
- providing tangible results

- vague audit scope definition
- poor audit preparation
- challenging communication

The Solution: EMERALD

How can EMERALD support me?

- Overview on automated vs. manual tests
- Enable manual result enrichment
- Guide testers with task lists
- Support custom tests and reuse

Figure 45. Persona-on-the-go for Eero – Technical Auditor

5.7.1 Scenario A: Eero – Technical Audit

For the technical audit, Eero needs to check the integrity and validity status of the results and tools and if the technical evidence is updated regularly (see Figure 58 in *APPENDIX B*). Eero trusts EMERALD and accesses the results of the controls that are not fulfilled (non-compliant, no result). They perform technical analysis with the tools and manual tests to then add the acquired knowledge to the audit report.

5.7.2 Scenario B: Eero – Reporting

Eero reports back to the lead auditor with his findings. They identified all non-compliances and created an audit report where they document and translate all non-compliances (see Figure 59 in *APPENDIX B: Original User Scenario Descriptions*).

6 UI/UX Requirements (version 2)

All requirements for the EMERALD UI/UX were elicited during all activities (e.g. interviews, focus groups, workshops…) that have been conducted in WP4. The goal of the requirements is to collect all features and needs of the pilot partners and component owners to design and develop the EMERALD UI, resulting in 25 requirements overall. All requirements have been added to the common Git repository of the EMERALD project. Every requirement was described with the following fields: Requirement Id, short title, description, status, priority, component, source, type, related KR, related KPI, and validation acceptance criteria. Additionally, we added information about the current progress status of the requirements regarding the clickable prototype of the EMERALD UI. The progress status of the requirements regarding the implementation of the UI have been reported in D4.5 (M15) [25] and will be reported in D4.6 (M27).

The related key result and KPI for all the UI/UX requirements are:

- **KR6: EMERALD UI/UX - User experience for complexity reduction:** A user interaction concept and conducted studies to show what information each user needs in an audit process. The concept shall lead to a user interface (UI), which is tailored to the users' needs during all stages of an audit and guides them through the process of identifying problems top-down – from high-level requirements down to specific implementation in documents (e.g., policies) or technical specifications [2].
- **KPI 6.3:** Provide a graphical user interface for role-based access to certification information content [2].

Table 13 provides an overview of all UI/UX requirements and the current progress regarding the implementation of the clickable prototype of the EMERALD UI.

All requirements that have been elicited before M9 have been presented using their full description in *APPENDIX C: UI/UX Requirements elicited before M9*. All newly elicited requirements since M9 are presented in Section 6.1.

Table 13. Status of the UI/UX requirements regarding the clickable prototype

ID	Short title	Description	Progress
UIUX.01	Landing Page	The landing page of the UI has to provide quick access to the following views: • Audit Scope Creation View • *MARI* Tool View • Certification Schemes Manager View	95% - Addressed – waiting for feedback and input from all EMERALD partners
UIUX.02	Audit Scope Creation View	There must be a view to create and save a new audit scope. This view allows to: • Setup a name for the audit scope • Select one of the available targets of evaluation • Select one of the available certification schemes • Upload policy documents The available targets of evaluation and certification schemes must be retrieved from the backend. Once the audit scope is saved, the policy documents must be uploaded to the backend.	90% - Mostly addressed - maybe some minor changes to come
UIUX.03	Controls Overview View	There must be a view where all the controls are presented. The controls must be fetched from the backend for the currently selected audit scope. For each control show: • ID • Description • Category • Person or department to whom the control is currently assigned • Compliance Compliance can be one of: • Compliant • Non-compliant	80% - The control overview view is there; it still needs to be decided which status information will be shown.
UIUX.04	Controls Overview View: Progress Indicators	On the Controls Overview View a chart must present the status and the compliance of the controls.	80% - The chart in the control overview view is there, but it still needs to be decided what to exactly show there.
UIUX.05	Controls Overview View: Filtering and Searching	It must be possible to filter the controls by each of the presented columns. It must also be possible to search for specific controls by entering either the ID or parts of the description.	100% - Addressed

ID	Short title	Description	Progress
UIUX.06	Policy Documents Manager View	There must be a view where users can manage (upload, remove) the policy documents.	90% - Still some minor things to implement
UIUX.07	Policy Documents Manager View: Metrics Selection	It should be possible to select one or more metrics per policy document. When extracting evidence from this document, the AMOE component should only consider the selected metrics.	100%
UIUX.08	Evidence Extractors View	There must be a view where users can see the status of the evidence extractors. This view must also allow to pause or enable existing ones. If one of the evidence extractors triggers an error, this should be presented here.	95% - Addressed - maybe some minor changes to come
UIUX.09	Control Detail View	There must be a view where the users can see all the details related to a single control. All the information available about the control should be listed here.	95% - Mostly addressed – it needs to be decided which information about the control should be presented.
UIUX.10	Control Detail View: Assignment	There must be an element, which the user can use to assign a control to another user or a department.	95% - Addressed – maybe some minor changes to come.
UIUX.11	Control Detail View: History	There must be a view, where the user can check the entire history of a control.	75% - Mostly addressed – it needs to be decided which information should be displayed there.
UIUX.12	Control Detail View: Evidence	There must be a view where the user can check the evidence gathered for the metrics of a control.	80% - Work in progress
UIUX.13	Control Detail View: Non-Compliance	There must be an explanation, why the current control is not compliant.	80% - Work in progress
UIUX.14	MARI Tool View	There must be a view, where the user can interact with the *MARI* tool.	95% - Addressed – maybe some minor changes to come
UIUX.15	Certification Schemes Manager View	There must be a view, where the user can see the available certification schemes.	95% - Addressed – maybe some minor changes to come
UIUX.16	Certification Schemes Manager View: BYOCS	On the Certification Schemes Manager View it should be possible to create a new certification scheme by selecting controls from existing certification schemes or by defining custom controls. (BYOCS = Bring Your Own Certification Scheme).	90% - Addressed - maybe some minor changes to come

ID	Short title	Description	Progress
UIUX.17	Certification Schemes Manager View: Import/Export	On the Certification Schemes Manager View it should be possible to import new certification schemes or to export existing ones via a CSV file or OSCAL format files.	90% - Import & Export Addressed - maybe some minor changes to come.
UIUX.18	Trustworthiness Check	The EMERALD UI should display a symbol to let the user know if the integrity of the evidence and/or assessments has been compromised. The integrity check should happen at regular intervals and can be manually triggered by the user.	100% - The symbol is available and allows the user to re-trigger the integrity check; if necessary, users can see and download a report containing the compromised evidence and/or assessments.
UIUX.19	Intuitive and Smooth UI	The EMERALD UI must be user-friendly and easy to use, so that all employees can understand it. The UI must allow to easily monitor compliance status across various targets of evaluation. Furthermore, the initial load of the UI should not exceed normal timing on a standard broadband connection and must respond to user actions within few seconds for all interactions.	70% - Work in progress
UIUX.20	Reusable metrics	It must be possible to reuse already-set-up metrics. The metrics must be suggested to the user, when a second certification scheme is looked at, so that the user does not have to remember that these metrics exist.	80% - Work in progress
UIUX.21	Transfer of Audit to EMERALD	The EMERALD UI should have a wizard or a workflow that helps new users to transfer current audit processes to EMERALD.	20% - Difficult
UIUX.22	Control Detail View: Manual Evidence	Controls that cannot be automatically assessed should have a field where the user can upload a file as evidence.	90% - Addressed
UIUX.23	Reporting	Users of the EMERALD UI can create different reports e.g., list of non-compliant controls, export into different formats (e.g. xlsx, pdf. docx).	0% - to be discussed
UIUX.24	UI Documentation	There should be a documentation (in form of text or videos) of the EMERALD UI in clear and understandable language so that users can easily understand the tool and the components to onboard tool administrators, compliance managers and other target users.	0% - to be discussed

ID	Short title	Description	Progress
UIUX.25	Self-Assessment Questionnaire for EUCS	There should be the possibility to perform a self-assessment (in the form of a questionnaire) of the fulfilment degree of the EUCS certification scheme for various levels (Basic, Substantial, and High) in the EMERALD UI. The questionnaire will allow users to answer a series of questions to evaluate the fulfilment of each control involved. It also provides the option for users to enter comments related to each question, as well as textual references to locate the evidence supporting the given answer. The system will generate a summary dashboard displaying quantitative values that reflect the degree of fulfilment for each level. Additionally, auditors will have access to the questionnaire, where they can review the self-assessment and enter non-conformities for any controls that are not fulfilled, providing a comprehensive overview of the certification status.	5% - Work in progress

6.1 Newly Added UI/UX Requirements since M9

Below we present the eight additional requirements for the EMERALD UI/UX, which have been added since M9. In this case we present the whole description and the status progress for the clickable prototype.

Field	Description
Requirement id	UIUX.18
Short title	Trustworthiness Check
Description	The EMERALD UI should display a symbol to let the user know if the integrity of the evidence and/or assessments has been compromised. The integrity check should happen at regular intervals and can be manually triggered by the user.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*TWS*
Source	Component
Type	GUI
Related KR	KR7_INTEROP
Related KPI	-
Validation acceptance criteria	The symbol should be visible and reflect the status of the integrity of the evidence and assessments. Furthermore, it must be possible to trigger a new check manually.
Progress	100% - The symbol is available and allows the user to re-trigger the integrity check; if necessary, users can see and download a report containing the compromised evidence and/or assessments.

Field	**Description**
Requirement id	UIUX.19
Short title	Intuitive and Smooth UI
Description	The EMERALD UI must be user-friendly and easy to use, so that all employees can understand it. The UI must allow to easily monitor compliance status across various targets of evaluation. Furthermore, the initial load of the UI should not exceed normal timing on a standard broadband connection and must respond to user actions within few seconds for all interactions.
Status	Proposed
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD UI/UX
Related KPI	KPI::6.3
Validation acceptance criteria	Validate the design by performing workshops with the target users.
Progress	70% - Work in progress

Field	**Description**
Requirement id	UIUX.20
Short title	Reusable metrics
Description	It must be possible to reuse already-set-up metrics. The metrics must be suggested to the user, when a second certification scheme is looked at, so that the user does not have to remember that these metrics exist.
Status	Implemented (in the clickable prototype)
Priority	Must
Component	*EmeraldUI, RCM, MARI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	Metrics that have already been set up, should be suggested to the user, when setting up a new certification scheme.
Progress	80% - Work in progress

Field	**Description**
Requirement id	UIUX.21
Short title	Transfer of Audit to EMERALD
Description	The EMERALD UI should have a wizard or a workflow that helps new users to transfer current audit processes to EMERALD.
Status	Proposed
Priority	Should
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD UI/UX

Related KPI	KPI 6.3
Validation acceptance criteria	The wizard/workflow is present and can be understood (validation via workshop) by new users.
Progress	20% - Difficult

Field	**Description**
Requirement id	UIUX.22
Short title	Control Detail View: Manual Evidence
Description	Controls that cannot be automatically assessed should have a field where the user can upload a file as evidence.
Status	Proposed
Priority	Should
Component	*EmeraldUI*, *Clouditor-Evidence Store*, *Clouditor-Assessment*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	It is possible to upload evidence files for manual controls.
Progress	90% - Addressed

Field	**Description**
Requirement id	UIUX.23
Short title	Reporting
Description	Users of the EMERALD UI can create different reports e.g., list of non-compliant controls, export into different formats (e.g. xlsx, pdf. docx).
Status	Proposed
Priority	Should
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6 EMERALD UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	Reports can be created and downloaded.
Progress	0% - to be discussed

Field	**Description**
Requirement id	UIUX.24
Short title	UI Documentation
Description	There should be a documentation (in form of text or videos) of the EMERALD UI in clear and understandable language so that users can easily understand the tool and the components to onboard tool administrators, compliance managers and other target users.
Status	Proposed
Priority	Should
Component	*EmeraldUI*

Source	Pilots
Type	GUI
Related KR	KR6_EMERALD UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	Documentation should cover all components of EMERALD as well as the tool itself in a clear and understandable language. Plausible Measurements: ▪ Review the documentation to ensure it includes detailed descriptions, usage guidelines, and interactions for each component in EMERALD. • Conduct usability tests/pilots with auditors to evaluate their understanding and ease of onboarding using the documentation and user manuals.
Progress	0% - to be discussed

Field	**Description**
Requirement id	UIUX.25
Short title	Self-Assessment Questionnaire for EUCS
Description	There should be the possibility to perform a self-assessment (in the form of a questionnaire) of the fulfilment degree of the EUCS certification scheme for various levels (Basic, Substantial, and High) in the EMERALD UI. The questionnaire will allow users to answer a series of questions to evaluate the fulfilment of each control involved. It also provides the option for users to enter comments related to each question, as well as textual references to locate the evidence supporting the given answer. The system will generate a summary dashboard displaying quantitative values that reflect the degree of fulfilment for each level. Additionally, auditors will have access to the questionnaire, where they can review the self-assessment and enter non-conformities for any controls that are not fulfilled, providing a comprehensive overview of the certification status.
Status	Proposed
Priority	Should
Component	*EmeraldUI*
Source	Component
Type	GUI
Related KR	KR6_EMERALD UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	Ensure users can answer questions, add comments and references, and save responses; verify the dashboard displays accurate fulfilment levels, auditors can review assessments and document non-conformities, and that auditors can track and resolve non-conformities effectively.
Progress	5% - Work in progress

7 Conclusions

This deliverable presents the results of task *T4.1 – Requirements engineering with compliance managers and auditors* and *T4.2 – Modelling work processes.* Therefore, it has presented the overall methodology used in WP4 and the results achieved by applying different methods in the context of the EMERALD project. In more detail:

- We derived first insights about the **pilots' audit preparation processes** in general, their **needs**, some **pain points** and **expectations** towards EMERALD. This was needed to get first ideas or insights on where the EMERALD UI could support them during the audit preparation and execution process.
- For each of the pilot partners and the auditors and compliance managers from NIXU/DNV we were able to derive **concrete work processes** about the audit preparation and the audit execution. These processes present the preparation and execution of audits from the perspective of compliance managers, security managers, and auditors including the working tasks, the information and data they need to do their tasks, and how the EMERALD solution could be used to support them.
- From the individual work processes, we developed a **universally applicable blueprint for implementing EMERALD** in audit preparation and audit execution workflows. This blueprint may be valuable for other companies seeking to use the EMERALD solution to enhance their audit preparation processes or to support audit executions.
- We derived seven personas divided into 3 different stakeholder groups – **3 personas** related to the **compliance stakeholders, one persona** related to the **technical stakeholders and 3 personas** related to **auditor stakeholders.** For these personas, we developed a **"persona-on-the-go"** and **18 detailed scenarios.** The personas and scenarios helped us to understand the roles and tasks of compliance managers, auditors, and technical stakeholders. This is essential for designing a system that effectively supports certification preparation and audit execution and for identifying the key functionalities needed in the EMERALD UI to support each stakeholder group.
- Finally, we were able to derive **25 UI/UX requirements** for developing the EMERALD UI.

T4.1 and T4.2 have ended in M18 of the EMERALD project. This means that we presented the final work processes, personas and scenarios, and the requirements. However, the work in WP4 will be continued using the results gained from T4.1 and T4.2. On the one hand, for T4.3 we will use the results to further develop the clickable prototype of EMERALD and bring it into a state that has implemented all requirements (to a certain extent). Additionally, we will ensure that the prototype supports the respective work processes and use the personas as baseline roles for the user administration in EMERALD, including to inform which user is allowed to do what in the EMERALD UI. On the other hand, the work for T4.3 is strongly aligned with T4.4, where the EMERALD UI will be implemented. Thus, results gained T4.3 that are based on T4.1 and T4.2 will directly be taken over in T4.4.

8 References

[1] EMERALD Consortium, “D4.1- Results of the UI-UX requirements analysis and the work processes - v1,” 2024.

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

[3] S. M. Dennerlein, V. Tomberg, T. Treasure-Jones, D. Theiler, S. Lindstaedt and T. Ley, “Co-designing tools for workplace learning: A method for analysing and tracing the appropriation of affordances in design-based research,” *Information and Learning Sciences,* vol. 121, no. 3/4, pp. 175-205, 2020.

[4] A. Fessl, V. Pammer-Schindler, K. Pata, S. Feyertag, M. Mõttus, J. Janus and T. Ley, “A Cooperative Design Method for SMEs to Adopt New Technologies for Knowledge Management: A Multiple Case Study,” *JUCS - Journal of Universal Computer Science,* vol. 26, no. 9, pp. 1189-1212, 2020.

[5] E. B.-N. Sanders and P. J. Stappers, “Co-creation and the new landscapes of design,” *CoDesign,* vol. 4, no. 1, pp. 5-18, 2008.

[6] F. Kensing and J. Blomberg, “Participatory Design: Issues and Concerns,” *Computer Supported Cooperative Work (CSCW),* vol. 7, no. 3, pp. 167-185, 1998.

[7] S. Bødker and K. Grønbæk, “Cooperative prototyping: users and designers in mutual activity,” *International Journal of Man-Machine Studies,* vol. 34, no. 3, pp. 453-478, 1991.

[8] EMERALD Consortium, “D4.3 – User interaction and user experience concept – v1,” 2024.

[9] EMERALD Consortium, “D7.2 Data Management Plan–v1,” 2024.

[10] J. Gläser and G. Laudel, Experteninterviews und qualitative Inhaltsanalyse, Springer-Verlag, 2010.

[11] D. L. Morgan, “Focus Groups,” *Annual Review of Sociology,* vol. 22, pp. 129-152, 1996.

[12] A. Cooper, “The Inmates are Running the Asylum,” in *Software-Ergonomie '99: Design von Informationswelten*, Wiesbaden, Vieweg+Teubner Verlag, 1999, pp. 17-17.

[13] T. Adlin and J. Pruitt, The Persona Lifecycle: Keeping People in Mind Throughout Product Design, Elsevier, 2006.

[14] P. Turner and S. Turner, “Is stereotyping inevitable when designing with personas?,” *Design Studies,* vol. 32, no. 1, pp. 30-44, 2011.

[15] T. Miaskiewicz and K. A. Kozar, “Personas and user-centered design: How can personas benefit product design processes?,” *Design Studies,* vol. 32, no. 5, pp. 417-430, 2011.

[16] A. Cooper, R. Reimann, D. Cronin and C. Noessel, About Face: The Essentials of Interaction Design, John Wiley & Sons, 2014.

[17] B. Martin and B. Hanington, Universal Methods of Design: 100 Ways to Research Complex Problems, Develop Innovative Ideas, and Design Effective Solutions, Rockport Publishers, 2012.

[18] EMERALD Consortium, "D5.1 Pilot definition, set-up & validation plan," 2024.

[19] C. Ashcraft, B. McLain and E. Eger, "Women in tech: The facts," National Center for Women & Technology, 2016.

[20] J. E. Fountain, "Constructing the information society: women, information technology, and design," *Technology in Society,* vol. 22, no. 1, pp. 45-62, 2000.

[21] J. Wajcman, "Reflections on Gender and Technology Studies," *Social Studies of Science,* vol. 30, pp. 447-464, 2000.

[22] M. R. Lopes and C. Vogel, "Gender Effects in Mobile Application Development," in *2020 IEEE International Conference on Human-Machine Systems*, New York, NY, USA, 2020.

[23] M. R. Lopes and C. Vogel, "The Influence of Personas' Gender in Design," in *Proceedings of the 14th Biannual Conference of the Italian SIGCHI Chapter*, Bolzano, Italy, 2021.

[24] K. Rasmussen et al., "Gender inclusive methods in studies of STEM practitioners," arXiv preprint arXiv:2307.15802, 2023.

[25] EMERALD Consortium, "D4.5 - EMERALD UI - v1," 2025.

[26] D. Long and B. Magerko, "What is AI Literacy? Competencies and Design Considerations," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu, HI, USA, 2020.

9 APPENDIX A: Interview Documents

The documents prepared for the interviews are presented. These documents consist of the interview guideline with the prepared questions, the participant information sheet covering all information an interview participant needs to know, a corresponding consent form that needs to be signed by the interview participants before the interview, and the data protection information. All prepared documents follow the GDPR guidelines and were checked by the Know-Center's legal department and the respective data protection officer.

9.1 Interview Guideline

Introduction

Short introduction of the interviewer – my name is Angela Fessl. I am ….

EMERALD is an HEU Project (GA no.: 101120688) with the objective to pave the road towards Compliance-as-a-Service (CaaS) for continuous certification of harmonized cybersecurity schemes like the EUCS. This interview is conducted within WP4 – User Interaction and User Experience development of the EMERALD Project. The goal of this interview is to elicit requirements from our target groups such as auditors/chief information security managers/compliance managers etc. necessary for developing the integrated EMERALD UI.

In more detail, our goal is to elicit in-depth insights about the work of [auditors/chief information security managers/compliance managers] in relation to continuous cloud auditing processes. Therefore, we are conducting a series of interviews aiming at getting …

- … a good understanding of your work in general,
- … your activities and tasks in the cloud computing systems certification process,
- … insights on how EMERALD could support your working activities,
- … insights about your expectations towards the EMERALD UI,
- … insights about existing pain points,
- (… and if you have been in the MEDINA project, what went good or not so good in MEDINA, and what could be done better or different in EMERALD)

The interview will cover the following topics:

- **General Information** about you and your work as [auditors/chief information security managers/compliance managers].
- [AUDITORS] The audit process of cloud computing systems and **used technologies** as an auditor including all relevant steps.
- [CISO] The **workflow** ensuring compliance for the cloud computing systems and **used technologies** as a chief information security manager, including all relevant steps.
- [CM] The **workflow** ensuring compliance for the cloud computing systems and **used technologies** as a compliance manager, including all relevant steps.
- How the **EMERALD technologies** can support the [audit process/ CISO-CM workflow].
- And which **AI literacy** related competences do [auditors/chief information security managers/compliance managers] need, to successfully conduct [audit process/ CISO-CM workflow] for could computing services.

Before we start, is it ok to record this interview?

General

At the beginning of the interview, I would like to know more about you and your company, as well as your role as [auditor/chief information security manager/compliance manager]. Additionally, I would like to know more about your responsibilities and what tasks are related to your [audit process/CISO-CM workflow].

- Please briefly describe who you are and what education you have.
- Please briefly describe the field of activity of your company.
- Please briefly describe your role in your company.
- And please describe your role as [auditor/chief information security manager/compliance manager]

Audit/CM Workflow and Technology Support

In this section, I would like to get more in-depth information about the [audit process/CISO-CM workflow].

Please shortly describe the [audit process/CISO-CM workflow] of cloud computing systems you are typically involved in – if possible, step by step.

- Please describe for each step, which information/data you need to have.
- Please describe for each step, which of the steps you do perform yourself and which of them are performed by your colleagues and why?
- What is the outcome of the [audit process/CISO-CM workflow]?
    - An audit report (auditor), a track record of evidence, …

- [Auditor question] What are the main objectives of auditing cloud computing systems from a compliance perspective?
- [Auditor question] How do you identify and assess risks associated with cloud computing systems during the audit process?
- [Auditor question] What are the key challenges you encounter when auditing cloud computing systems for compliance?

- [CISO/CM question] What are the main objectives when preparing for an audit of cloud computing systems?
- [CISO/CM question] What are the key challenges you encounter when preparing for an audit?
- [CISO/CM question] Do you continuously monitor for compliance? If so, how?

- What happens when non-compliance is detected?
- Which tools, software, framework do you use for which step in the [audit process/CISO-CM workflow]?
- Which data/information do the tools provide for which step?
- What are current pain points and challenges regarding the audit process / CM process?
- How do you ensure the accuracy and reliability of the information collected during the audit process?

EMERALD Project Results / EMERALD Technologies

The goal of the EMERALD project is to provide evidence management for continuous certification as a service in the cloud. EMERALD leverages the findings of the well esteemed H2020 project MEDINA, starting from TRL 5 in summer 2023 and advances them in the EMERALD Core to

TRL 7. EMERALD will focus on evidence management components for the continuous certification approach. EMERALD will provide a proof of concept (PoC) for mapping the findings to future AI certification schemes.

- Think about how new technologies including AI could help you in improving the [audit process/CISO-CM workflow]?
  - What would be helpful for you in general?
  - What could be useful features?
  - Which information / data should such a tool provide for your work?
  - Are there specific tasks or areas within the audit process where AI could provide the most value?
- Thinking now explicitly about EMERALD, how could EMERALD support you during the [audit process/CISO-CM workflow]?
  - What must EMERALD provide to you to make EMERALD successful for you?

The Role of AI in Audit Processes

If you think now about the [audit process/CISO-CM workflow] for the cloud computing systems, it is important to take into consideration that an AI-based tool supporting them needs to be trustworthy – thus you need to trust them. In this regard, the EC has defined 7 key requirements that AI systems should meet in order to be considered as trustworthy. We will not address all of them during this interview, but at least those that are relevant for the development of the EMERALD UI/UX.

Show prepared slide set with definitions.

Therefore, from your opinion and perspective:

- How can the transparency and interpretability of AI algorithms used in the [audit process/CISO-CM workflow] be ensured?
- What measures should be implemented to address potential biases or ethical concerns in AI-based auditing systems?

AI Literacy

In the last section, we would like to know from your perspective, which AI Literacy Skills a [auditor/chief information security manager/compliance manager] must have, to reliably be able to thoroughly conduct the [audit process/CISO-CM workflow]

Do you know the term “AI Literacy”?

“AI literacy as a set of competencies that enables individuals to critically evaluate AI technologies; communicate and collaborate effectively with AI; and use AI as a tool online, at home, and in the workplace.” [26]

- What do you associate with the term AI / artificial intelligence?
  - From which sources do you get your knowledge about AI?
- Which AI technologies do you know or use?
  - Do you have a basic understanding of the mathematical models underlying ML models?
- What level of AI literacy or familiarity with AI technologies do you believe is necessary for auditors to effectively utilize AI tools or systems in the audit process for cloud computing systems?
- How do you currently address any gaps in AI literacy among [auditor/chief information security manager/compliance manager] within your organization or team?

- Which strategies do you employ to enhance your understanding or the understanding of your colleagues of AI technologies relevant to auditing?

Closing

This is already the end of the interview.

- Is there any additional information or insights you would like to share regarding auditing cloud computing systems or the role of AI in the audit process?

Thank you for your time and valuable input.

9.2 Participant Information Sheet

Introduction

You are invited to participate in an interview study related to the EMERALD Project. Before deciding on whether you want to participate or not, please read the information below. Please ask the researcher all the questions you may have so you are completely sure that you understand all the proceedings of the study. The contact details are provided at the end of this information sheet.

Purpose of the study

EMERALD is an HEU Project (GA no.: 101120688) with the objective to pave the road towards Compliance-as-a-Service (CaaS) for continuous certification of harmonized cybersecurity schemes like the EUCS. This interview is conducted within WP4 – User Interaction and User Experience Development of the EMERALD Project. The goal of this interview is to elicit requirements of [auditors/chief information security managers/compliance managers] necessary for developing the integrated EMERALD UI.

In more detail, our goal is to elicit in-depth insights about your work as [auditors/chief information security managers/compliance managers] in relation to continuous cloud auditing processes. Therefore, we are conducting a series of interviews aiming at getting …

- … a good understanding of your work in general,
- … your activities and tasks in the cloud computing systems certification process,
- … insights on how EMERALD could support your working activities,
- … insights about the expectations towards the EMERALD UI,
- … insights about existing pain points,
- (… and if you have been in the MEDINA project, what went good or not so good in MEDINA, and what could be done better or different in EMERALD)

Your participation in the study

You are invited to participate in this study on a voluntary basis and you are free to withdraw from the study at any time without providing any reason for doing so. If you agree to participate in this interview, you give us permission to:

- Collect information from you
- Share information (only answers you provide without any personal information) with the people of the project
- Conduct the study
- Use this information in the analysis and for publication.

Benefits of the participation

It is likely that you might not receive any direct personal benefit for your participation in this interview besides possibly learning more about the EMERALD project in general. However, by participating you will make a substantial contribution to the success of the EMERALD project, as we need your expertise for developing a good and easy-to-use EMERALD UI/UX that supports you during your work.

Disadvantages and/or risks of the participation

No risk is foreseen. You are only requested to be available to participate.

Confidentiality and publication of the study data

Any responses you provide in the interview can be recorded or written down. The data, however, will not include any personal identification; hence it will not be possible to identify you afterwards. All the data you provide will be anonymised and treated confidentially. The information you provide will be analysed and presented in project reports together with the information from other participants. The raw data will be stored in the internal servers of the Know-Center protected by passwords that are only known to researchers conducting the interview. All the raw data will be stored for 5 years after the project finalisation.

Funding of the research

The research leading to this interview has received funding from the European Union's Horizon Europe Research and Innovation Programme, under Grant Agreement no 101120688.

Contact for further information or in case of withdrawal from the study

DI Dr. Angela Fessl, Know-Center GmbH, afessl@know-center.at

9.3 Consent Form

Background of this study

EMERALD is a Horizon Europe Project (GA no.: 101120688) with the objective to pave the road towards Compliance-as-a-Service (CaaS) for continuous certification of harmonized cybersecurity schemes like the EUCS. This interview is conducted within WP4 – User Interaction and User Experience development of the EMERALD Project. The goal of this interview is to elicit requirements from our target groups such as auditors/chief information security managers/compliance managers etc. necessary for developing the integrated EMERALD UI. In more detail, our goal is to elicit in-depth insights about your work as auditors/chief information security managers/compliance managers in relation to continuous cloud auditing processes.

Statement of researcher's responsibility

As researcher, I have explained the nature of this research study and the procedures to be undertaken in this context. I have offered to answer any questions and fully answered such questions.

Declaration of participant

I confirm that: I am 18 years old or older and I am competent to provide consent. I have read and understood the information about this study, as provided in the Information Sheet. I have also had the opportunity to ask questions, and all my questions have been answered to my satisfaction. I freely and voluntarily agree to participate in this research study. I understand that I may refuse to answer any question and that I may withdraw at any time without being penalised for withdrawing nor questioned on why I have withdrawn. I agree that my personal information will remain confidential and that my data will be used anonymously and securely in research and publications, in a way that my identity cannot be revealed. I understand that other researchers will have access to this data only if they agree to preserve the confidentiality of the data.
I agree to the terms and to the recording of the consent procedure/ and interview (phone interviews)

Participant:

__________________________ __________________________________ __________________

Name Signature Date

Researcher:

__________________________ __________________________________ __________________

Name Signature Date

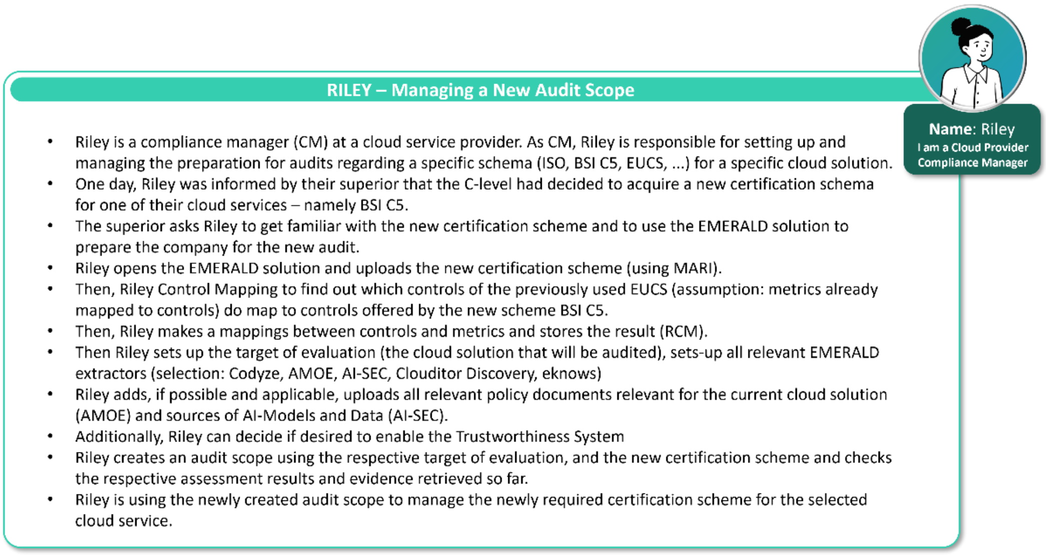
9.4 Data Protection Information

Controller:	Know-Center GmbH Research Center for Data Driven Business & Big Data Analytics, Sandgasse 36/4, 8010 Graz Contact: info@know-center.at
Data protection officer:	Data Protection Officer of Know-Center GmbH Sandgasse 34/4, 8010 Graz Contact: datenschutz@know-center.at
Purpose of processing:	Maintaining business contacts to the extent that this is covered by the reasons for being contacted to which the data subject has consented.
Data:	Name, e-mail address, relevant for contacting the interview partners to which they have given their consent.
Basis in law:	Consent pursuant to GDPR Art 6 (1) (a)
Recipient:	No transmission to third parties; no contract processing
Transmission to third countries:	No
Duration of storage:	Until the time when you withdraw your consent. Irrespective of withdrawal of consent, the data will be deleted if your e-mail address becomes invalid or if we receive notification that communications are undeliverable.
Data subject rights:	You have the right to: - **Information and access**, to find out whether we have personal data of yours stored and what data it is. - **Rectification – correction and/or completion** of your personal data that are incorrect or incomplete - **Erasure – deletion** of your personal data that are being processed in a manner which is not lawful or is no longer lawful - **Restriction of processing** - **Data portability** - **Withdraw consent** that you have given, effective for the future: i.e., further processing of your data is then not allowed from that point in time onwards, unless there is an overriding legitimate reason for doing so. - **Object** to any assertion by Know-Center GmbH of an overriding legitimate interest in storing/processing the data To exercise these rights please contact datenschutz@know-center.at. You also have a right to make a **complaint to the Data Protection Authority**. In this regard, we also refer to their homepage, which can be accessed under the link https://www.dsb.gv.at

10 APPENDIX B: Original User Scenario Descriptions

In the following sections we included all user scenario descriptions that have not been adapted. The adaptation of the user scenarios took place if there was an adaption needed based on the technical feasibility in EMERALD.

10.1 Scenarios Riley

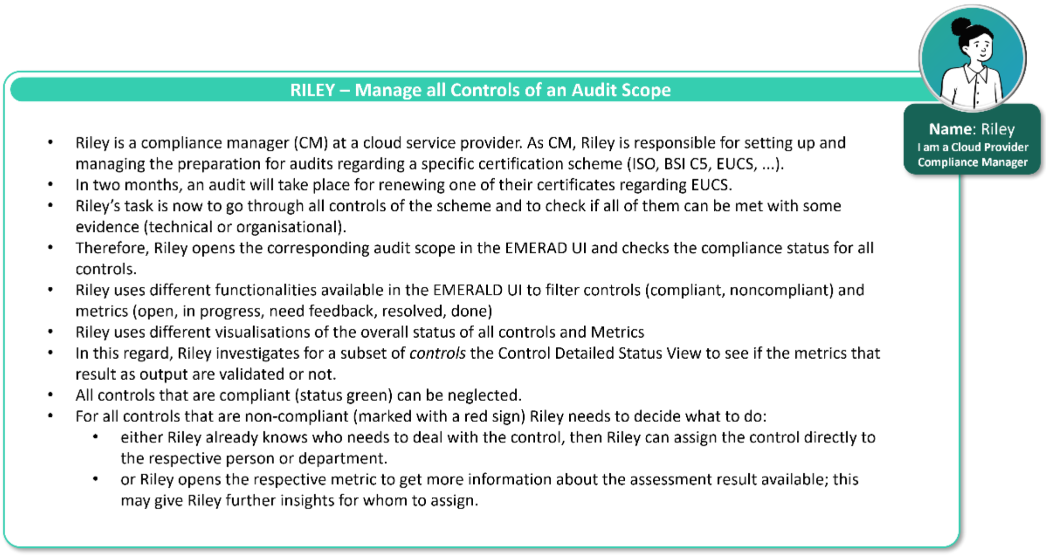


RILEY – Managing a New Audit Scope

Name: Riley
I am a Cloud Provider Compliance Manager

- Riley is a compliance manager (CM) at a cloud service provider. As CM, Riley is responsible for setting up and managing the preparation for audits regarding a specific schema (ISO, BSI C5, EUCS, …) for a specific cloud solution.
- One day, Riley was informed by their superior that the C-level had decided to acquire a new certification schema for one of their cloud services – namely BSI C5.
- The superior asks Riley to get familiar with the new certification scheme and to use the EMERALD solution to prepare the company for the new audit.
- Riley opens the EMERALD solution and uploads the new certification scheme (using MARI).
- Then, Riley Control Mapping to find out which controls of the previously used EUCS (assumption: metrics already mapped to controls) do map to controls offered by the new scheme BSI C5.
- Then, Riley makes a mappings between controls and metrics and stores the result (RCM).
- Then Riley sets up the target of evaluation (the cloud solution that will be audited), sets-up all relevant EMERALD extractors (selection: Codyze, AMOE, AI-SEC, Clouditor Discovery, eknows)
- Riley adds, if possible and applicable, uploads all relevant policy documents relevant for the current cloud solution (AMOE) and sources of AI-Models and Data (AI-SEC).
- Additionally, Riley can decide if desired to enable the Trustworthiness System
- Riley creates an audit scope using the respective target of evaluation, and the new certification scheme and checks the respective assessment results and evidence retrieved so far.
- Riley is using the newly created audit scope to manage the newly required certification scheme for the selected cloud service.

Figure 46. Scenario A: Riley – Manging a new audit scope

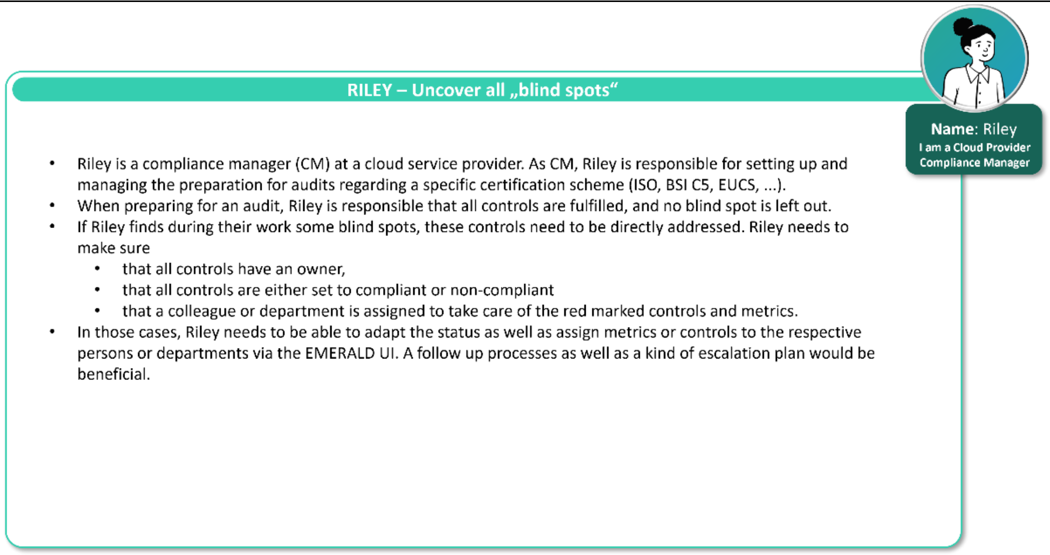


RILEY – Manage all Controls of an Audit Scope

Name: Riley
I am a Cloud Provider Compliance Manager

- Riley is a compliance manager (CM) at a cloud service provider. As CM, Riley is responsible for setting up and managing the preparation for audits regarding a specific certification scheme (ISO, BSI C5, EUCS, …).
- In two months, an audit will take place for renewing one of their certificates regarding EUCS.
- Riley's task is now to go through all controls of the scheme and to check if all of them can be met with some evidence (technical or organisational).
- Therefore, Riley opens the corresponding audit scope in the EMERAD UI and checks the compliance status for all controls.
- Riley uses different functionalities available in the EMERALD UI to filter controls (compliant, noncompliant) and metrics (open, in progress, need feedback, resolved, done)
- Riley uses different visualisations of the overall status of all controls and Metrics
- In this regard, Riley investigates for a subset of *controls* the Control Detailed Status View to see if the metrics that result as output are validated or not.
- All controls that are compliant (status green) can be neglected.
- For all controls that are non-compliant (marked with a red sign) Riley needs to decide what to do:
  - either Riley already knows who needs to deal with the control, then Riley can assign the control directly to the respective person or department.
  - or Riley opens the respective metric to get more information about the assessment result available; this may give Riley further insights for whom to assign.

Figure 47. Scenario B: Riley – Manage all Controls of an Audit Scope

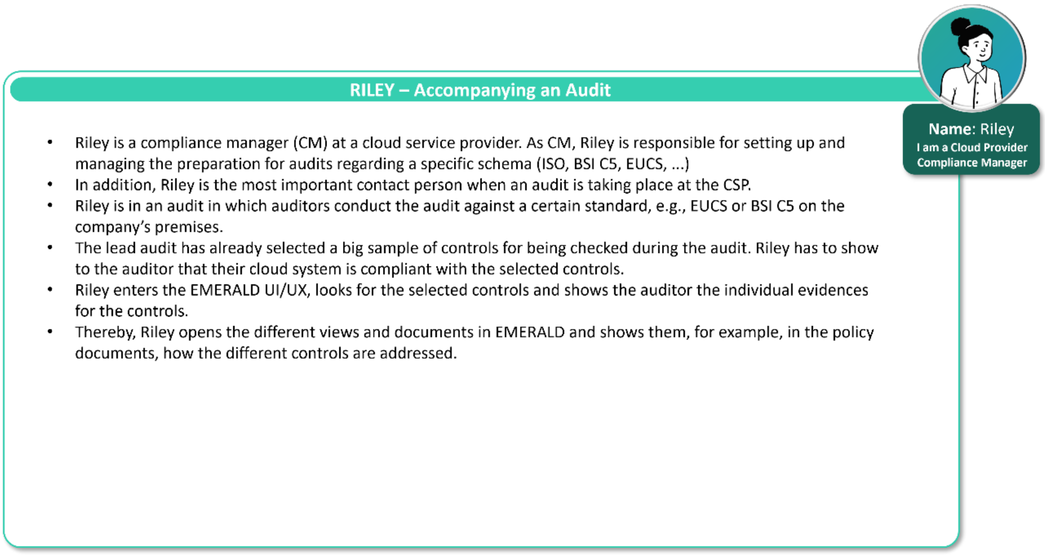


RILEY – Uncover all „blind spots"

Name: Riley
I am a Cloud Provider Compliance Manager

- Riley is a compliance manager (CM) at a cloud service provider. As CM, Riley is responsible for setting up and managing the preparation for audits regarding a specific certification scheme (ISO, BSI C5, EUCS, ...).
- When preparing for an audit, Riley is responsible that all controls are fulfilled, and no blind spot is left out.
- If Riley finds during their work some blind spots, these controls need to be directly addressed. Riley needs to make sure
  - that all controls have an owner,
  - that all controls are either set to compliant or non-compliant
  - that a colleague or department is assigned to take care of the red marked controls and metrics.
- In those cases, Riley needs to be able to adapt the status as well as assign metrics or controls to the respective persons or departments via the EMERALD UI. A follow up processes as well as a kind of escalation plan would be beneficial.

Figure 48. Scenario C: Riley – Uncover all "blind spots"



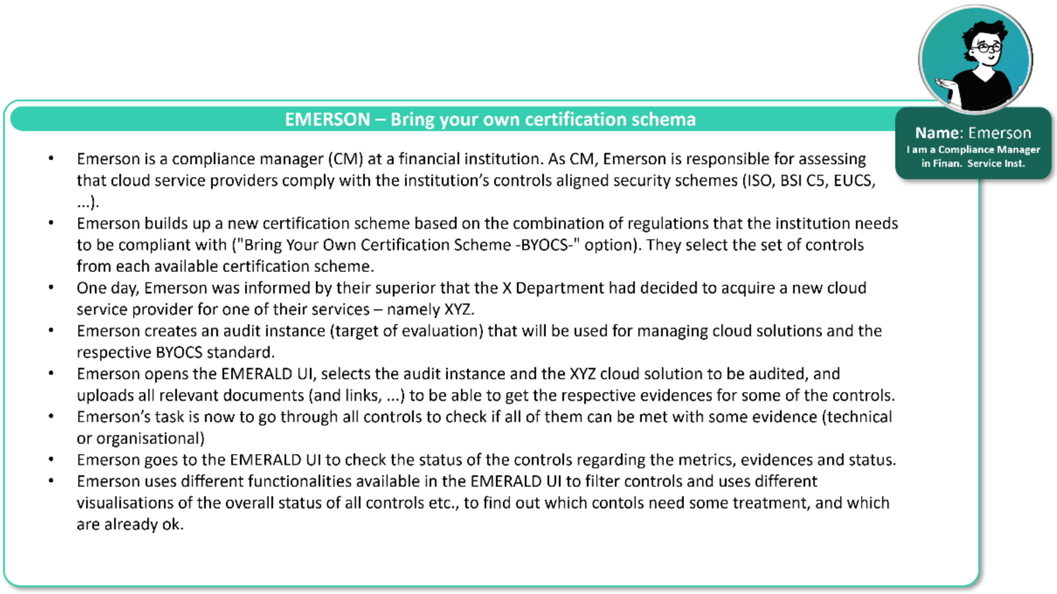
RILEY – Accompanying an Audit

Name: Riley
I am a Cloud Provider Compliance Manager

- Riley is a compliance manager (CM) at a cloud service provider. As CM, Riley is responsible for setting up and managing the preparation for audits regarding a specific schema (ISO, BSI C5, EUCS, ...)
- In addition, Riley is the most important contact person when an audit is taking place at the CSP.
- Riley is in an audit in which auditors conduct the audit against a certain standard, e.g., EUCS or BSI C5 on the company's premises.
- The lead audit has already selected a big sample of controls for being checked during the audit. Riley has to show to the auditor that their cloud system is compliant with the selected controls.
- Riley enters the EMERALD UI/UX, looks for the selected controls and shows the auditor the individual evidences for the controls.
- Thereby, Riley opens the different views and documents in EMERALD and shows them, for example, in the policy documents, how the different controls are addressed.

Figure 49. Scenario E: Riley – Accompanying and audit

10.2 Scenario Emerson



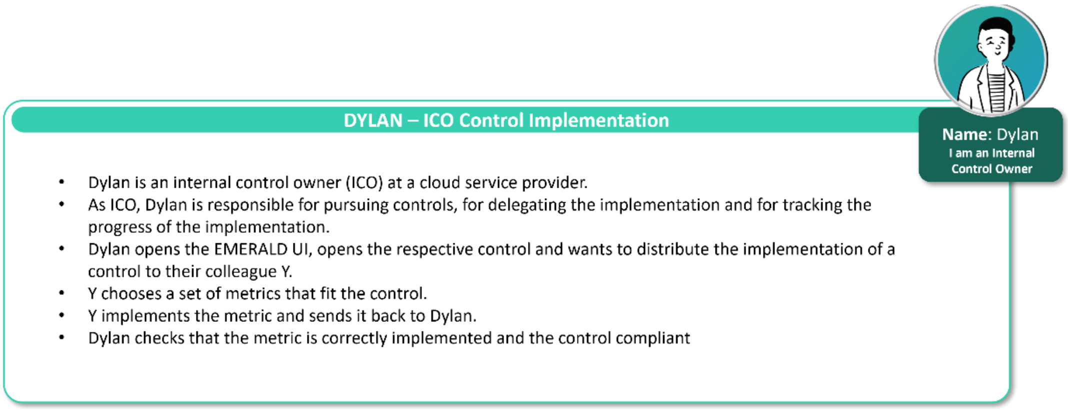
EMERSON – Bring your own certification schema

Name: Emerson
I am a Compliance Manager in Finan. Service Inst.

- Emerson is a compliance manager (CM) at a financial institution. As CM, Emerson is responsible for assessing that cloud service providers comply with the institution's controls aligned security schemes (ISO, BSI C5, EUCS, ...).
- Emerson builds up a new certification scheme based on the combination of regulations that the institution needs to be compliant with ("Bring Your Own Certification Scheme -BYOCS-" option). They select the set of controls from each available certification scheme.
- One day, Emerson was informed by their superior that the X Department had decided to acquire a new cloud service provider for one of their services – namely XYZ.
- Emerson creates an audit instance (target of evaluation) that will be used for managing cloud solutions and the respective BYOCS standard.
- Emerson opens the EMERALD UI, selects the audit instance and the XYZ cloud solution to be audited, and uploads all relevant documents (and links, ...) to be able to get the respective evidences for some of the controls.
- Emerson's task is now to go through all controls to check if all of them can be met with some evidence (technical or organisational)
- Emerson goes to the EMERALD UI to check the status of the controls regarding the metrics, evidences and status.
- Emerson uses different functionalities available in the EMERALD UI to filter controls and uses different visualisations of the overall status of all controls etc., to find out which contols need some treatment, and which are already ok.

Figure 50. Emerson – Bring your own certification scheme

10.3 Scenario Dylan



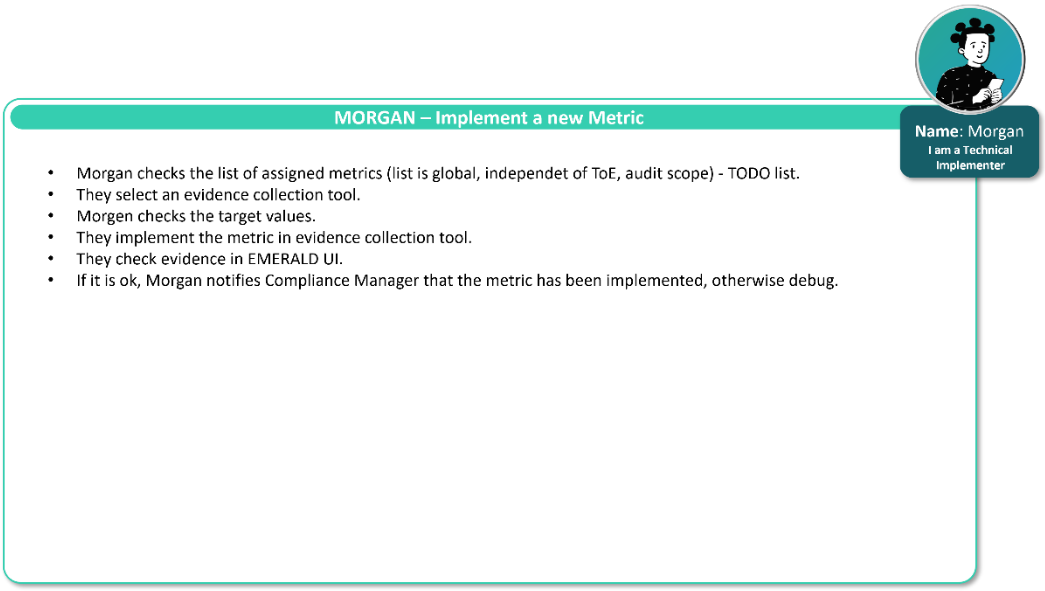
DYLAN – ICO Control Implementation

- Dylan is an internal control owner (ICO) at a cloud service provider.
- As ICO, Dylan is responsible for pursuing controls, for delegating the implementation and for tracking the progress of the implementation.
- Dylan opens the EMERALD UI, opens the respective control and wants to distribute the implementation of a control to their colleague Y.
- Y chooses a set of metrics that fit the control.
- Y implements the metric and sends it back to Dylan.
- Dylan checks that the metric is correctly implemented and the control compliant

Name: Dylan
I am an Internal Control Owner

Figure 51. Dylan – Internal Control Owner Control Implementation

10.4 Scenario Morgan



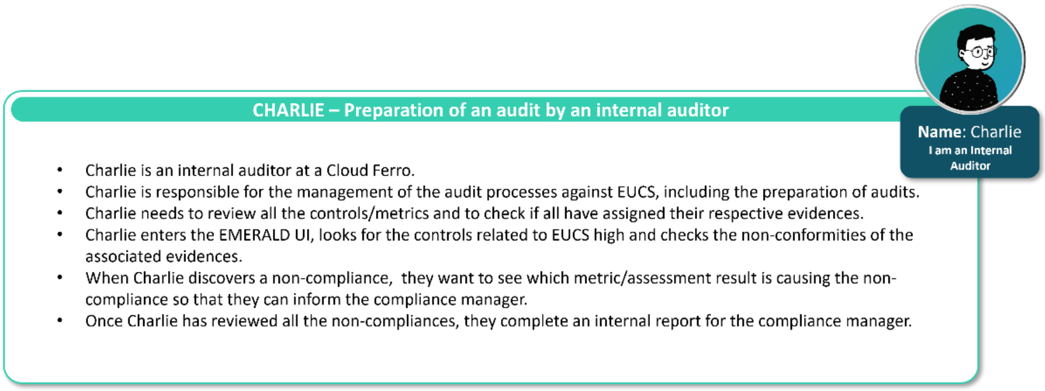
MORGAN – Implement a new Metric

- Morgan checks the list of assigned metrics (list is global, independet of ToE, audit scope) - TODO list.
- They select an evidence collection tool.
- Morgen checks the target values.
- They implement the metric in evidence collection tool.
- They check evidence in EMERALD UI.
- If it is ok, Morgan notifies Compliance Manager that the metric has been implemented, otherwise debug.

Name: Morgan
I am a Technical Implementer

Figure 52. Scenario A: Morgan – Checking Metrics and Evidence

10.5 Scenario Charlie



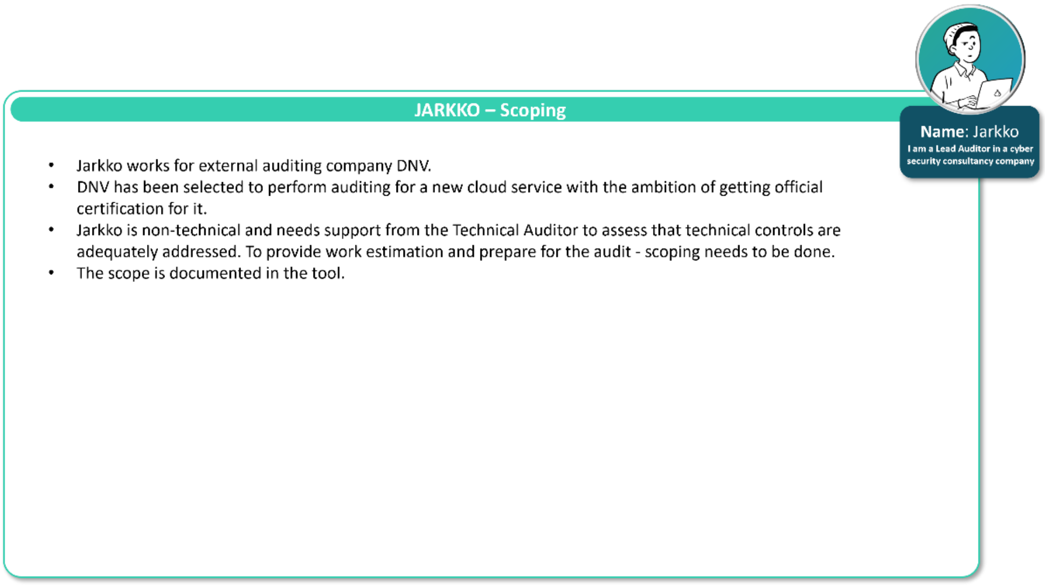
CHARLIE – Preparation of an audit by an internal auditor

- Charlie is an internal auditor at a Cloud Ferro.
- Charlie is responsible for the management of the audit processes against EUCS, including the preparation of audits.
- Charlie needs to review all the controls/metrics and to check if all have assigned their respective evidences.
- Charlie enters the EMERALD UI, looks for the controls related to EUCS high and checks the non-conformities of the associated evidences.
- When Charlie discovers a non-compliance, they want to see which metric/assessment result is causing the non-compliance so that they can inform the compliance manager.
- Once Charlie has reviewed all the non-compliances, they complete an internal report for the compliance manager.

Name: Charlie
I am an Internal Auditor

Figure 53. Scenario 3: Charlie – Preparation of an audit by an internal auditor

10.6 Scenarios Jarkko

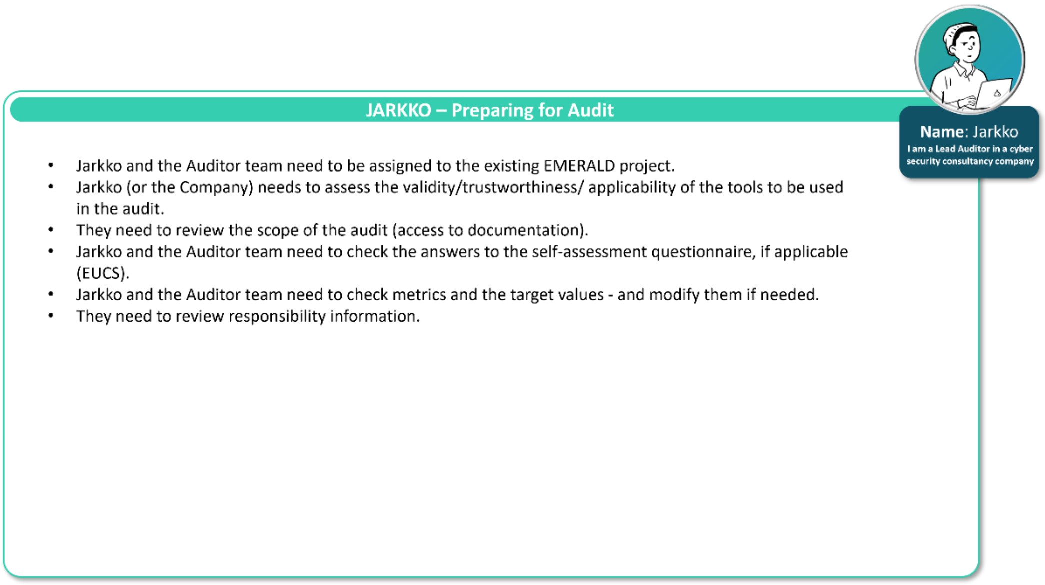


JARKKO – Scoping

Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company

- Jarkko works for external auditing company DNV.
- DNV has been selected to perform auditing for a new cloud service with the ambition of getting official certification for it.
- Jarkko is non-technical and needs support from the Technical Auditor to assess that technical controls are adequately addressed. To provide work estimation and prepare for the audit - scoping needs to be done.
- The scope is documented in the tool.

Figure 54. Scenario A: Jarkko – Scoping

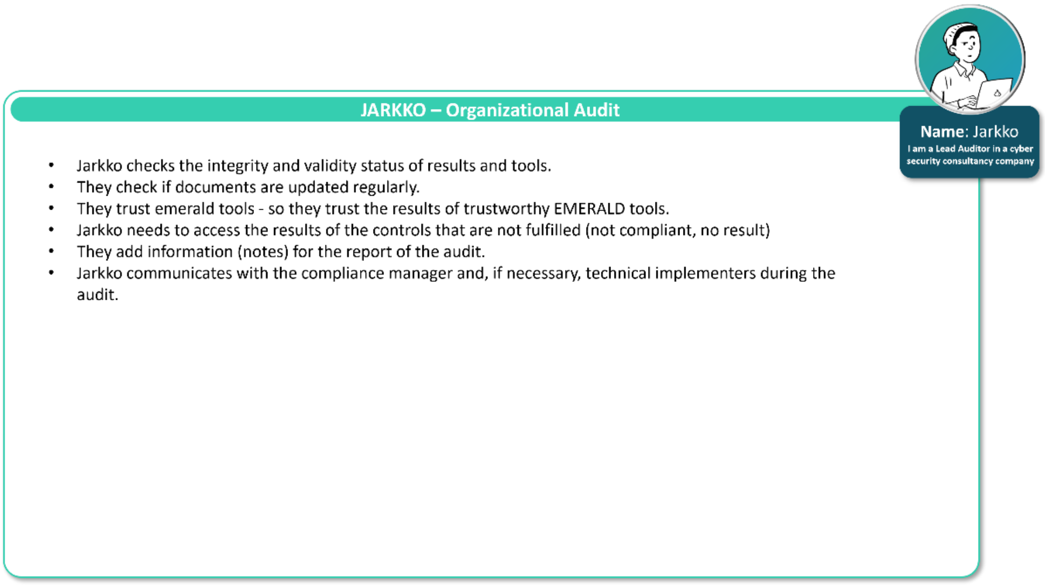


JARKKO – Preparing for Audit

Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company

- Jarkko and the Auditor team need to be assigned to the existing EMERALD project.
- Jarkko (or the Company) needs to assess the validity/trustworthiness/ applicability of the tools to be used in the audit.
- They need to review the scope of the audit (access to documentation).
- Jarkko and the Auditor team need to check the answers to the self-assessment questionnaire, if applicable (EUCS).
- Jarkko and the Auditor team need to check metrics and the target values - and modify them if needed.
- They need to review responsibility information.

Figure 55. Scenario B: Jarkko – Preparing for audit

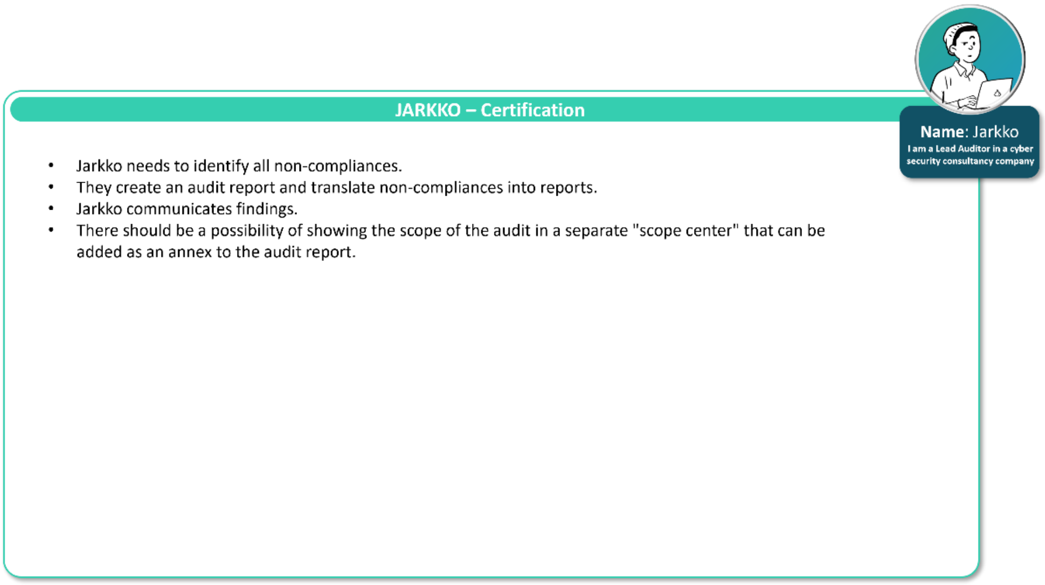


JARKKO – Organizational Audit

Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company

- Jarkko checks the integrity and validity status of results and tools.
- They check if documents are updated regularly.
- They trust emerald tools - so they trust the results of trustworthy EMERALD tools.
- Jarkko needs to access the results of the controls that are not fulfilled (not compliant, no result)
- They add information (notes) for the report of the audit.
- Jarkko communicates with the compliance manager and, if necessary, technical implementers during the audit.

Figure 56. Scenario C: Jarkko – Organizational Audit



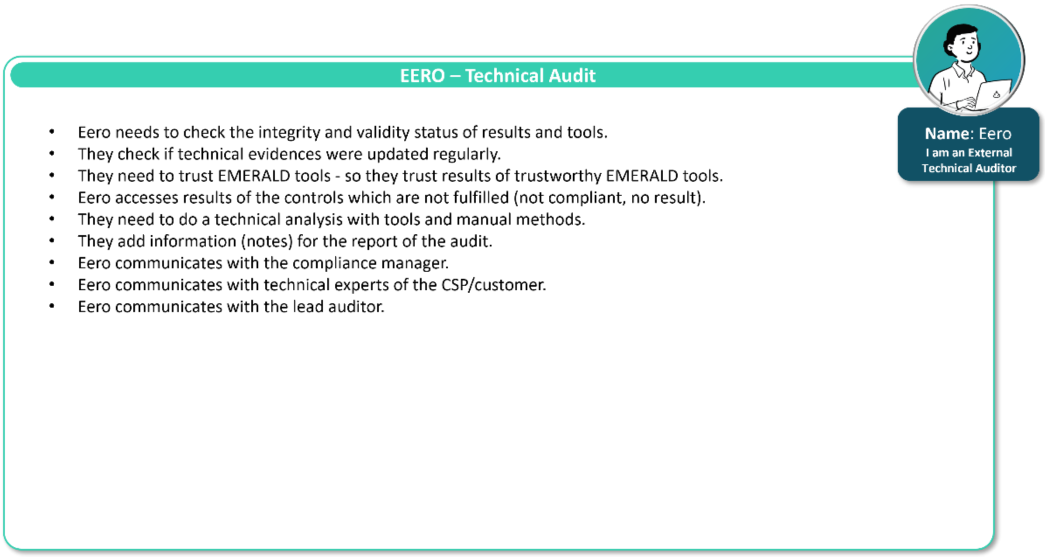
JARKKO – Certification

Name: Jarkko
I am a Lead Auditor in a cyber security consultancy company

- Jarkko needs to identify all non-compliances.
- They create an audit report and translate non-compliances into reports.
- Jarkko communicates findings.
- There should be a possibility of showing the scope of the audit in a separate "scope center" that can be added as an annex to the audit report.

Figure 57. Scenario D: Jarkko - Certification

10.7 Scenarios Eero

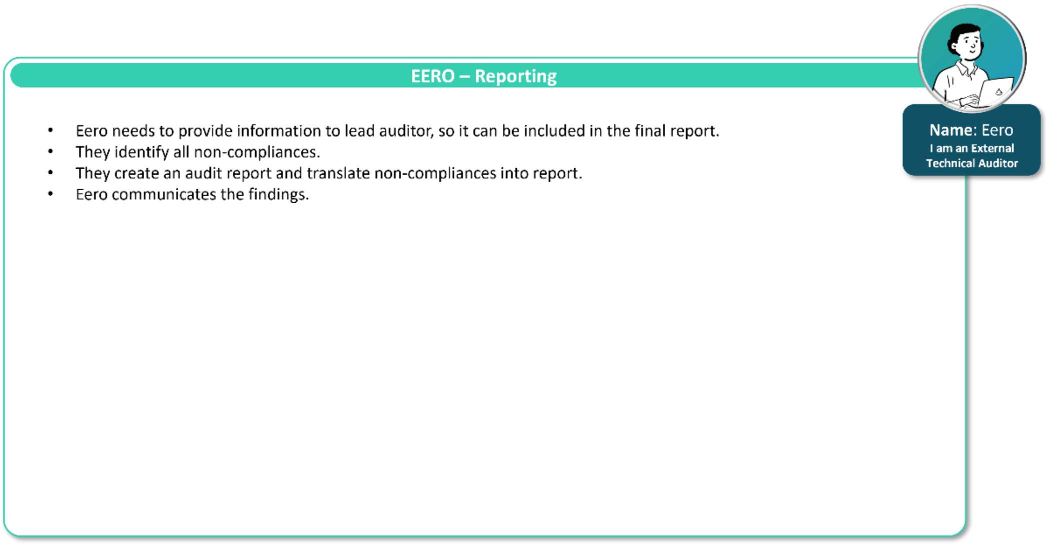


EERO – Technical Audit

- Eero needs to check the integrity and validity status of results and tools.
- They check if technical evidences were updated regularly.
- They need to trust EMERALD tools - so they trust results of trustworthy EMERALD tools.
- Eero accesses results of the controls which are not fulfilled (not compliant, no result).
- They need to do a technical analysis with tools and manual methods.
- They add information (notes) for the report of the audit.
- Eero communicates with the compliance manager.
- Eero communicates with technical experts of the CSP/customer.
- Eero communicates with the lead auditor.

Name: Eero
I am an External Technical Auditor

Figure 58. Scenario A: Eero – Technical Audit



EERO – Reporting

- Eero needs to provide information to lead auditor, so it can be included in the final report.
- They identify all non-compliances.
- They create an audit report and translate non-compliances into report.
- Eero communicates the findings.

Name: Eero
I am an External Technical Auditor

Figure 59. Scenario B: Eero - Reporting

11 APPENDIX C: UI/UX Requirements elicited before M9

Below we present the requirements for the EMERALD UI/UX which were elicited before M9. In this case we present the whole description and the status progress for the clickable prototype.

Field	**Description**
Requirement id	UIUX.01
Short title	Landing Page
Description	The landing page of the UI has to provide quick access to the following views: • Audit Instance Creation View • MARI Tool View • Certification Schemes Manager View
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The desired views can be reached from the landing page of the EMERALD UI.

Field	**Description**
Requirement id	UIUX.02
Short title	Audit Instance Creation View
Description	There must be a view to create and save a new audit instance. This view allows to: • Set a name for the audit instance • Select one of the available cloud services or add a new one • Select one of the available certification schemes or create a new one • Upload policy documents The available cloud services and certification schemes must be retrieved from the backend. Once the instance is saved, the policy documents must be uploaded to the backend.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, Orchestrator*
Source	KPI
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view allows to create a new audit instance with the desired fields and the instance is saved in the backend.

Field	Description
Requirement id	UIUX.03
Short title	Requirements Overview View
Description	There must be a view where all the requirements are presented. The requirements must be fetched from the backend for the currently selected audit instance. For each requirement the view will show: • ID • Description • Owner • Person or department to whom the requirement is currently assigned • Compliance • Status Compliance can be one of: • Compliant • Non-compliant Status can be one of: • Open • Need for discussion • Waiting for input • Waiting for confirmation by CM • Verified
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, RCM, Clouditor-Orchestrator*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	All the requirements of the scheme are displayed with the required information.

Field	Description
Requirement id	UIUX.04
Short title	Requirements Overview View: Progress Indicators
Description	On the Requirements Overview View a chart must present the status and the compliance of the requirements.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The chart is visible and updated correctly whenever there is a change in the requirements.

Field	**Description**
Requirement id	UIUX.05
Short title	Requirements Overview View: Filtering and Searching
Description	It must be possible to filter the requirements by each of the presented columns. It must also be possible to search for specific requirements by entering either the ID or parts of their description.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The filtering and searching functions work correctly and deliver the correct results.

Field	**Description**
Requirement id	UIUX.06
Short title	Policy Documents Manager View
Description	There must be a view where users can manage (upload, remove, replace) the policy documents.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, AMOE*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view is present and allows to perform the desired actions.

Field	**Description**
Requirement id	UIUX.07
Short title	Policy Documents Manager View: Metrics Selection
Description	It should be possible to select one or more metrics per policy document. When extracting evidence from this document, the AMOE component should only consider the selected metrics.
Status	Implemented (in clickable prototype)
Priority	Should
Component	*EmeraldUI, AMOE*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The metrics can be selected and AMOE analyses the documents using only the desired metrics.

Field	Description
Requirement id	UIUX.08
Short title	Evidence Extractors View
Description	There must be a view where users can see the status of the evidence extractors. This view must also allow to connect/add a new extractor, delete or disable existing ones. If one of the evidence extractors triggers an error, this should be presented here.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view is present and allows to interact with the evidence extractors.

Field	Description
Requirement id	UIUX.09
Short title	Requirement Detail View
Description	There must be a view where the users can see all the details related to a single requirement. All the information available about the requirement should be listed here.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The desired requirement is correctly displayed with all the corresponding information.

Field	Description
Requirement id	UIUX.10
Short title	Requirement Detail View: Assignment
Description	There must be a view where the user can assign a requirement to another user or a department.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present, and the requirement is assigned correctly.

Field	**Description**
Requirement id	UIUX.11
Short title	Requirement Detail View: History
Description	There must be a view, where the user can check the entire history of a requirement.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present, and the history must contain the correct data.

Field	**Description**
Requirement id	UIUX.12
Short title	Requirement Detail View: Evidence
Description	There must be a view, where the user can check, add or remove evidence for a specific requirement.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, AMOE, Evidence-Store*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present, and the user can check, add or remove evidence for the given requirement.

Field	**Description**
Requirement id	UIUX.13
Short title	Requirement Detail View: Non-Compliance
Description	There must be a view, where it is explained why the current requirement is not compliant.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI*
Source	Pilots
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present and the reason for non-compliance is explained.

Field	Description
Requirement id	UIUX.14
Short title	MARI Tool View
Description	There must be a view, where the user can interact with the MARI tool.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, MARI*
Source	Component
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present, and it must be possible to interact with the MARI tool.

Field	Description
Requirement id	UIUX.15
Short title	Certification Schemes Manager View
Description	There must be a view where the user can see the available certification schemes.
Status	Implemented (in clickable prototype)
Priority	Must
Component	*EmeraldUI, RCM*
Source	DoA
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	The view must be present and the available certification schemes displayed.

Field	Description
Requirement id	UIUX.16
Short title	Certification Schemes Manager View: BYOCS
Description	On the Certification Schemes Manager View it should be possible to create a new certification scheme by selecting requirements from existing certification schemes or by defining custom requirements.
Status	Implemented (in clickable prototype)
Priority	Should
Component	*EmeraldUI, Clouditor-Orchestrator, RCM*
Source	Pilot
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	It is possible to create a new certification scheme by selecting existing requirements or by adding custom requirements. The new certification scheme is then available to use in audit instances.

Field	**Description**
Requirement id	UIUX.17
Short title	Certification Schemes Manager View: Import/Export
Description	On the Certification Schemes Manager View it should be possible to import new certification schemes or to export existing ones via a CSV file.
Status	Implemented (in clickable prototype)
Priority	Could
Component	*EmeraldUI, Clouditor-Orchestrator, RCM*
Source	Pilot
Type	GUI
Related KR	KR6_EMERALD_UI/UX
Related KPI	KPI 6.3
Validation acceptance criteria	It is possible to import or export the desired certification scheme using a CSV file.