



EMERALD

Deliverable D4.1

Results of the UI-UX requirements analysis and the work processes – v1

Editor(s):	Angela Fessler, Simone Franza, Leonie Disch
Responsible Partner:	Know-Center GmbH
Status-Version:	Final v1.0
Date:	31.07.2024
Type:	R
Distribution level (SEN, PU):	PU

Project Number:	101120688
Project Title:	EMERALD

Title of Deliverable:	D4.1 Results of the UI-UX requirements analysis and the work processes–v1
Due Date of Delivery to the EC	31.07.2024

Workpackage responsible for the Deliverable:	WP4 - User interaction and user experience development
Editor(s):	Angela Fessler, Simone Franza, Leonie Disch (KNOW)
Contributor(s):	Björn Fanta, Franz Deimling, Olivia Kagerer, Lukas Ruckenstuhl (FABA) Maria Barros Weiss (IONOS) Ramon Martin de Pozuelo, Marti Fabregat I Pous (CXB) Natalia Sobieska (CF) Jordi Guijarro (ONS)
Reviewer(s):	Olivia Kagerer (FABA) Cristina Martínez, Juncal Alonso (TECNALIA)
SAB Reviewers:	Samu Nisula (NIXU) Constantino Vázquez (ONS) Mario Maawad (CXB) Daniela Greb (FABA) Tomasz Aniszewski (CF) Ali Nikouka (IONOS)
Approved by:	All Partners
Recommended/mandatory readers:	WP1, WP2, WP3, WP5, WP6

Abstract:	Initial version of the report on the elicited UI-UX requirements from the target groups. Work processes and workflows that should be covered with the user interface concept.
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	21.06.2024	First draft version	Angela Fessler (KNOW)
v0.1	26.06.2024	QA review	Olivia Kagerer (FABA)
v0.2	10.07.2024	Addressing the comments from the QA review	Angela Fessler, Simone Franza (KNOW)
v0.3	19.07.2024	Addressing the comments from the SAB review	Angela Fessler, Simone Franza (KNOW)
v0.4	22.07.2024	Submission of D4.1 for TECNALIA Review	Angela Fessler, Simone Franza (KNOW)
v0.5	25.07.2024	Addressing the comments from TECNALIA Review	Angela Fessler, Leonie Dish (KNOW)
v1.0	31.07.2024	Submitted to the European Commission	Cristina Martínez (TECNALIA)

Table of contents

Terms and abbreviations.....	6
Executive Summary.....	7
1 Introduction.....	8
1.1 About this deliverable.....	8
1.2 Document structure.....	9
2 Methodology.....	10
2.1 Interactive Interview Session.....	11
2.1.1 Procedure.....	11
2.2 Interviews.....	11
2.2.1 Procedure.....	12
2.3 Focus Groups.....	12
2.3.1 Procedure.....	13
2.4 Personas & Scenarios Workshop.....	13
2.4.1 Procedure.....	14
2.4.2 Gender-bias in Personas and Scenarios.....	16
3 Results of the Interactive Interview Session.....	17
4 Work Processes.....	21
4.1 Work Processes of Compliance and Security Managers per Pilot.....	21
4.1.1 Pilot 2: CloudFerro.....	21
4.1.2 Pilot 3: Fabasoft.....	23
4.1.3 Compliance Manager from NIXU.....	25
4.2 Work Processes of Auditors.....	26
5 Personas & Scenarios.....	30
5.1 Personas.....	30
5.1.1 Emerson - Compliance Manager in Financial Service Institution.....	30
5.1.2 Riley – Cloud Service Compliance Manager.....	31
5.1.3 Dylan – Internal Control Owner.....	32
5.1.4 Charlie - Auditor.....	33
5.2 Scenarios.....	34
5.2.1 Scenario 1: Emerson – Bring Your Own Certification Scheme.....	34
5.2.2 Scenario 2: Dylan – Internal Control Owner Requirement Implementation.....	35
5.2.3 Scenario 3: Charlie – Preparation of an Audit by an Internal Auditor.....	35
6 UI/UX Requirements (version 1).....	37
7 Conclusions.....	45
8 References.....	46
9 APPENDIX A: Interview Documents.....	48

9.1 Interview Guideline	48
9.2 Participant Information Sheet	51
9.3 Consent Form.....	53
9.4 Data Protection Information.....	54

List of Tables

TABLE 1. OVERVIEW OF THE CONDUCTED AND PLANNED INTERVIEWS	12
TABLE 2. OVERVIEW OF THE CONDUCTED AND PLANNED FOCUS GROUPS.....	13
TABLE 3. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q1: “HOW DO THE CURRENT AUDIT PROCESSES LOOK LIKE FOR YOUR PILOT?”	17
TABLE 4. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q2: “WHAT ARE THE “PAIN POINTS” FOR YOUR CURRENT AUDIT PROCESS?”	18
TABLE 5. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q3: “ARE THERE ANY SPECIFIC TASKS TO BE SOLVED BY EMERALD?”	18
TABLE 6. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q4: “HOW CAN EMERALD HELP MITIGATE THESE “PAIN POINTS”? EXPECTATIONS?”	19
TABLE 7. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q5: “WHAT TOOLS ARE YOU CURRENTLY USING FOR THE AUDITS IN YOUR PILOT?”	20
TABLE 8. SUMMARY OF ANSWERS GIVEN TO THE QUESTION Q6: “WHICH CERTIFICATION SCHEMES ARE YOU AS PILOT INTERESTED IN?”	20

List of Figures

FIGURE 1. OVERALL METHODOLOGY APPLIED IN WP4.....	10
FIGURE 2. PERSONA TEMPLATE.....	15
FIGURE 3. INDIVIDUAL PHASES OF AN AUDIT PREPARATION PROCESS OF A COMPLIANCE MANAGER AND SECURITY MANAGER FROM CLOUDFERRO	22
FIGURE 4. POTENTIAL SUPPORT OF THE COMPLIANCE MANAGER AND MAYBE SECURITY MANAGER OF CLOUDFERRO DURING AN AUDIT PREPARATION PROCESS WITH THE EMERALD UI.....	23
FIGURE 5. INDIVIDUAL PHASE OF AN AUDIT PREPARATION PROCESS OF A COMPLIANCE MANAGER FROM FABASOFT	24
FIGURE 6. POSSIBLE SUPPORT OF THE COMPLIANCE MANAGER OF FABASOFT DURING AN AUDIT PREPARATION PROCESS WITH THE EMERALD UI.....	24
FIGURE 7. INDIVIDUAL PHASE OF AN AUDIT PREPARATION PROCESS OF A COMPLIANCE MANAGER (BLUE) ORGANIZED BY NIXU AND POSSIBLE EMERALD SUPPORT (ORANGE)	26
FIGURE 8. INDIVIDUAL PHASES FOR CONDUCTING AUDIT PROCESSES OF IN GENERAL (BLUE) AND ENHANCED FOR CLOUD SOLUTIONS (GREEN)	28
FIGURE 9. POSSIBLE SUPPORT OF THE AUDIT PROCESS WITH THE EMERALD UI/UX.....	29
FIGURE 10. PERSONA EMERSON – COMPLIANCE MANAGER IN FINANCIAL SERVICE INSTITUTION	31
FIGURE 11. PERSONA RILEY – COMPLIANCE MANAGER OF A CLOUD PROVIDER	32
FIGURE 12. PERSONA DYLAN – INTERNAL CONTROL OWNER	33
FIGURE 13. PERSONA CHARLIE - AN (INTERNAL) AUDITOR	34
FIGURE 14. SCENARIO 1: EMERSON – BRING YOUR OWN CERTIFICATION SCHEME	35
FIGURE 15. SCENARIO 2: DYLAN – INTERNAL CONTROL OWNER REQUIREMENT IMPLEMENTATION.....	35
FIGURE 16. SCENARIO 3: CHARLIE - PREPARATION OF AN AUDIT BY AN INTERNAL AUDITOR	36

Terms and abbreviations

A	Auditor
AI	Artificial Intelligence
AI4C	Criteria Catalogue for AI Cloud Services
AMOE	Assessment and Management of Organisational Evidence
BYOCS	Bring Your Own Certification Scheme
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
C5	Cloud Computing Compliance Criteria Catalogue
CaaS	Certification-as-a-service
CISO	Chief Information Security Manager
CM	Compliance Manager
CIS	Center for Internet Security
CSV	Comma-separated value
DoA	Description of Action
DORA	Digital Operational Resilience Act
ECB	European Central Bank
ENS	National Security Framework (Esquema Nacional de Seguridad)
EUCS	European Union Cybersecurity Certification Scheme for Cloud Services
GA	Grant Agreement to the project
ICO	Internal Control Owner
GUI	Graphical User Interface
ISO	International Organization for Standardization
GUI	Graphical User Interface
KPI	Key Performance Indicator
KR	Key Result
MARI	Mapping Assistant for Regulations with Intelligence
RCM	Repository of Controls and Metrics
SAB	Security Advisory Board
TRL	Technology Readiness Level
UI	User Interface
UX	User Experience

Executive Summary

The EMERALD UI/UX (user interface/user experience) offers the user interface (UI) and user experience (UX) to address certification-as-a-service (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 in the end leads to a fully-fledged UI/UX for EMERALD.

This deliverable D4.1 is related to *WP4 - User interaction and user experience development* and presents first results regarding *T4.1 - Requirements engineering with compliance managers and auditors* and *T4.2 - Modelling work processes*. The document describes the applied methodology and the requirement analysis conducted so far, as well as the first results derived, namely the initial work processes and the first set of concrete UI/UX requirements relevant for implementing the EMERALD UI/UX.

In more detail, this deliverable presents the results of the interactive interview session to get insights about the pilot partners' needs, the initially elicited work processes, the first set of personas and corresponding scenarios, and the elicited UI/UX requirements. The main findings can be summarized as follows:

- From the interactive interview session at the general assembly in Bilbao, Spain (March 2024), we were able to derive insights about the **pilots' audit preparation processes** in general, their **needs**, some **pain points** and some **expectations** regarding EMERALD.
- From the 7 interviews and 2 focus groups conducted so far, we were able to **derive initial concrete work processes** per pilot and for external auditors regarding the preparation and conduction of audits from the perspective of compliance managers, security managers and auditors.
- From the Personas and Scenarios workshop that was conducted in June 2024, we derived four personas – **2 different compliance manager personas**, **1 internal control owner persona**, and **1 auditor persona**. Additionally, we developed **6 general scenarios** and **3 detailed scenarios** to understand the work of compliance managers, internal control owners and auditors in more detail.
- Finally, we were able to derive an initial set of **17 UI/UX requirements** for developing the EMERALD UI/UX.

In the upcoming months, we will continue with the activities to be able to provide at the end of M18 the final versions of the work processes, personas and scenarios, and a complete set of UI/UX requirements for the EMERALD UI/UX. Therefore, a subsequent version of this document (D4.2) will be released in M18, where the final results of T4.1 and T4.2 will be presented.

1 Introduction

The EMERALD UI/UX offers the user interface (UI) and user experience (UX) to address certification-as-a-service (CaaS) and its continuous and lean re-certification aspects with a focus on the user's needs. The user experience (UX) describes the quality of the experience the target users have with a specific product or service, while the user interface (UI) represents the design and layout of the product or service. UI and UX are closely linked to each other, with a seamless UI design playing a crucial role in shaping a positive and efficient UX.

This deliverable describes the applied methodology and the requirement analysis conducted so far, as well as the first results derived, namely the initial derived work processes and the first set of concrete UI/UX requirements relevant for implementing the EMERALD UI/UX. Therefore, different methods were applied, and different studies were conducted to elicit which information the target users need to have during an audit process or for preparing an audit. The developed EMERALD UI/UX will be tailored to the users' needs to support them during all stages of an audit and to guide 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.

This section introduces the context of this deliverable regarding the EMERALD project, the aim and audience of the content as well as the document structure. This deliverable presents the initial results of task *T4.1 – Requirements engineering with compliance managers and auditors* and *T4.2 – Modelling work processes*, as both tasks will continue until M18 of the EMERALD project. The final results of both tasks will be summarised in D4.2, to be released in M18.

1.1 About this deliverable

One of the project's objectives as defined in the DoA [1] 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.” [2]

In this deliverable, we describe the methodological approach used to reach this objective and present the first concrete results of T4.1 and T4.2. All results are preliminary and will be continuously further developed, updated, and validated until M18 of the project.

Different methods have been used and applied to meet the EMERALD project context regarding the UI/UX development, and consists of three major elements:

- **Methodology:** The overall methodology was used to derive the initial set of UI/UX requirements and the initial work processes of the target groups. This overall methodology consisted of different interviews, focus groups, and the first persona & scenario workshop.
- **Work Processes:** From the interviews, focus groups, and the persona & scenario workshop, a first set of work processes was derived.
- **UI/UX Requirements:** Finally, 17 UI/UX requirements were derived. 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: The technical partners, because their components and the corresponding outputs will be connected to and presented in the EMERALD UI. The pilot partners, as their employees including compliance managers, internal control owners and auditors, are the target groups of the EMERALD project.
- Second, this document is also targeted to the broader EMERALD target users (e.g., potential end-users, strategic partners, communities, or policymakers) who are interested in socio-technical design, co-creation and co-design. For them, it will provide some guidance and concrete examples on how to elicit knowledge from people with different backgrounds (e.g., interviews, focus groups), and 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 and requirement analysis conducted so far, as well as the initial versions of the work processes and workflows elicited from the target groups. Furthermore, we present the first derived set of UI/UX requirements necessary for the future EMERALD UI/UX development.

1.2 Document structure

The document is structured as follows:

After the introduction section, Section 1, Section 2 presents the overall methodology used for fulfilling the objectives of Tasks 4.1 and 4.2. Subsequently, it includes a separate section for each step of the methodology to present its results.

Section 3 summarizes the findings of the interactive interview session held at the general assembly in Bilbao. Section 4 presents the initial versions of the work processes elicited so far from the interviews and focus groups conducted with the pilot partners. Section 5 consolidates the findings from the first workshop on personas and scenarios. Section 6 presents the initial set of UI/UX requirements we have derived from all the activities conducted (e.g., interviews, focus groups, workshops). Finally, Section 7 concludes the report and presents the next steps.

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

2 Methodology

The overall methodology of WP4 follows a co-design, participatory and contextual design approach (see [3], [4], [5], and [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. Originating from the collaboration between designers and end-users, this approach shifted the focus from merely creating products to addressing users' needs [6]. 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.

The goal of applying co-design as overall methodology for the WP4 activities was seen as a viable mean to bridge the gap between the EMERALD technology partners and the EMERALD pilot partners to be able to develop a sophisticated EMERALD UI/UX that meets the needs of both sides. Thereby, the aim of the co-design is: i) to get a good understanding of the underlying processes and workflows regarding the preparation and conduction of audits and certification of cloud services, ii) to start with the elicitation of requirements for the development of the EMERALD UI/UX, iii) to begin with the development of personas and scenarios, and iv) to develop first prototypes and mock-ups. The elicitation process is conducted in an iterative way to continuously involve the target groups throughout the different activities and processes, to gather their feedback and insights and to allow for their input to be integrated on-the-fly.

Subsequently, the methodology was followed, as depicted in Figure 1. First, an interactive interview session was conducted at the first face-to-face general assembly in Bilbao in March 2024, the results of which are presented in Section 3. This was followed by semi-structured interviews with the target users, including auditors, compliance managers, and security managers from the different pilot partners, followed by online focus groups. The goal was to elicit the respective work processes, which are summarised in Section 4. After the first round of interviews and focus groups, an online workshop was conducted in June 2024 for the development of scenarios and personas, the results of which are presented in Section 5.

In parallel and based on all collected insights gained from the activities conducted so far, a set of 17 UI/UX requirements for developing the EMERALD UI/UX were derived, which are presented in Section 6.

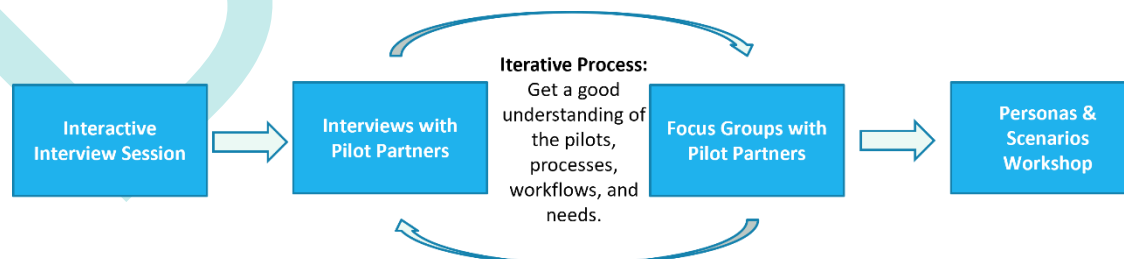


Figure 1. Overall methodology applied in WP4

The following subsections present the methods used and the procedures applied in the different activities.

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 needs during the set-up and conduction of audit processes, and to get first ideas or insights 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?

2.1.1 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 present 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 is to elicit requirements for the EMERALD UI/UX from our target groups. In the context of EMERALD [1], the target groups are, on the one hand, the pilot partners and, in particular, those employees who have to deal with the preparation and fulfilment of cybersecurity standards in the respective organisations. These employees consist of (internal) auditors, chief information security managers, compliance 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.

In more detail, the goal of the interviews is to elicit in-depth insights about the work of auditors (A), compliance managers (CM), and (chief information) security managers (CISO) 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) about the users’ background knowledge, especially regarding artificial intelligence (AI) (as some parts of EMERALD will use AI technologies).

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. In order to comply with the current GDPR regulations, 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 subsequently 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 [8].

2.2.1 Procedure

To invite our respective target groups, we contacted the EMERALD pilot partners and asked them to put 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 question. 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 in a written way – meaning that CaixaBank received the interview guideline from us and collected the answers from its Information Security Governance team in a written way.

The analysis of the collected primary data was carried out in the form of qualitative content analysis following Glaeser and Laudel [9]. 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 as preparation for the planned focus groups (see Section 2.3).

So far, we have already conducted 7 interviews with compliance managers, security managers and auditors as depicted in Table 1.

Table 1. Overview of the conducted and planned interviews

Pilot	Participants	Type
IONOS	<ul style="list-style-type: none"> 1 interview with a Leader of the Security Management Team 	Online in MS Teams
	<ul style="list-style-type: none"> 1 interview to come 	
CloudFerro	<ul style="list-style-type: none"> 1 Interview with a Compliance Manager 	Online in MS Teams
	<ul style="list-style-type: none"> 1 Interview with a Security Manager 	Online in MS Teams
Fabasoft	<ul style="list-style-type: none"> 1 Interview with 3 Compliance Managers 	Online in MS Teams
	<ul style="list-style-type: none"> 1-2 interviews to come 	
CaixaBank	<ul style="list-style-type: none"> 1 (written) interview with the Information Security Governance team 	Written interview answers
NIXU	<ul style="list-style-type: none"> 1 Interview with 3 Auditors 	Online in MS Teams
	<ul style="list-style-type: none"> 1 interview with a Compliance Manager 	Online in MS Teams

2.3 Focus Groups

Complementing the interviews, we conducted a focus group per pilot, in which all interviewees from the pilot participated, to discuss in-depth the derived results and to correct possible misunderstandings.

Focus groups can typically be seen as group interviews, but guided by specific triggers for discussion [10]. In our case, the triggers were the consolidated results of the individual interviews. The results 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 EMERALD UI could offer support.

2.3.1 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 findings from the interviews. Additionally, the participants were asked to go through the slide set before the focus group was scheduled in order to be prepared to provide us with valuable feedback and further information of 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, all gained feedback and input was integrated into the developed slide set and then sent out again to the respective focus group participants.

So far, we have conducted 2 focus groups as depicted in Table 2.

Table 2. Overview of the conducted and planned focus groups

Pilot	Participants	Type
IONOS	<ul style="list-style-type: none"> 1 focus group to come 	
CloudFerro	<ul style="list-style-type: none"> 1 focus group to come 	
Fabasoft	<ul style="list-style-type: none"> 1 focus group with 1 compliance manager and 1 consortium member 	Online in MS Teams
CaixaBank	<ul style="list-style-type: none"> 1 focus group to come 	
NIXU	<ul style="list-style-type: none"> 1 focus group with 1 compliance manager and the NIXU project manager from the consortium 	Online in MS Teams

2.4 Personas & Scenarios Workshop

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/UX and which functionalities should be available. Further workshops of this type will be organised.

Personas are a goal-directed design tool introduced by Cooper [11]. A persona typically represents a fictional individual or a representative group of persons with similar characteristics (see [12], [13]). They are often described in a narrative way to make the person seem real and to provide needs of these individuals in the related context [14]. Personas are typically used in combination with scenarios. Scenarios describe, in a narrative way, how target users will ideally interact with the developed technology [15]. After having developed personas and scenarios, user journeys [16] are another design method to help understand the interaction between a user and a technology. User journeys show step by step the user's interaction with the system and should include emotions [16]. They help to determine which requirements the planned technology – in our case the EMERALD UI/UX – must or should have. However, the user journeys and the resulting interactions with the paper-based mock-ups will not be presented in this deliverable, but in the upcoming deliverable D4.3 (M12).

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 workshop should help to 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 to gather information on the functionalities to be provided by the EMERALD UI.

2.4.1 Procedure

In order to invite participants to the workshop, we contacted the pilot partners and all members of WP4 and WP5 by email. The Personas & Scenarios Workshop was conducted online using MS Teams. To facilitate collaboration, we used Miro¹, an online collaborative whiteboard.

The workshop was conducted on two different days, i.e., in two parts as described below.

Workshop Part I: The first part of the workshop was attended by 11-14 participants. The agenda was as follows: first, we gave an introduction about 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 shortly note down their expectations towards the workshop. Afterwards, we presented a summary of how the work processes elicited from the different pilot partners' interviews looked like. 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.

Figure 2 shows the persona template which consist 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.

As a result, four different personas were developed (see Section 5.1):

- Emerson - Compliance Manager in Financial Services
- Riley – Cloud Provider Compliance Manager
- Dylan – Internal Control Owner
- Charlie – Auditor

¹ <https://miro.com/>

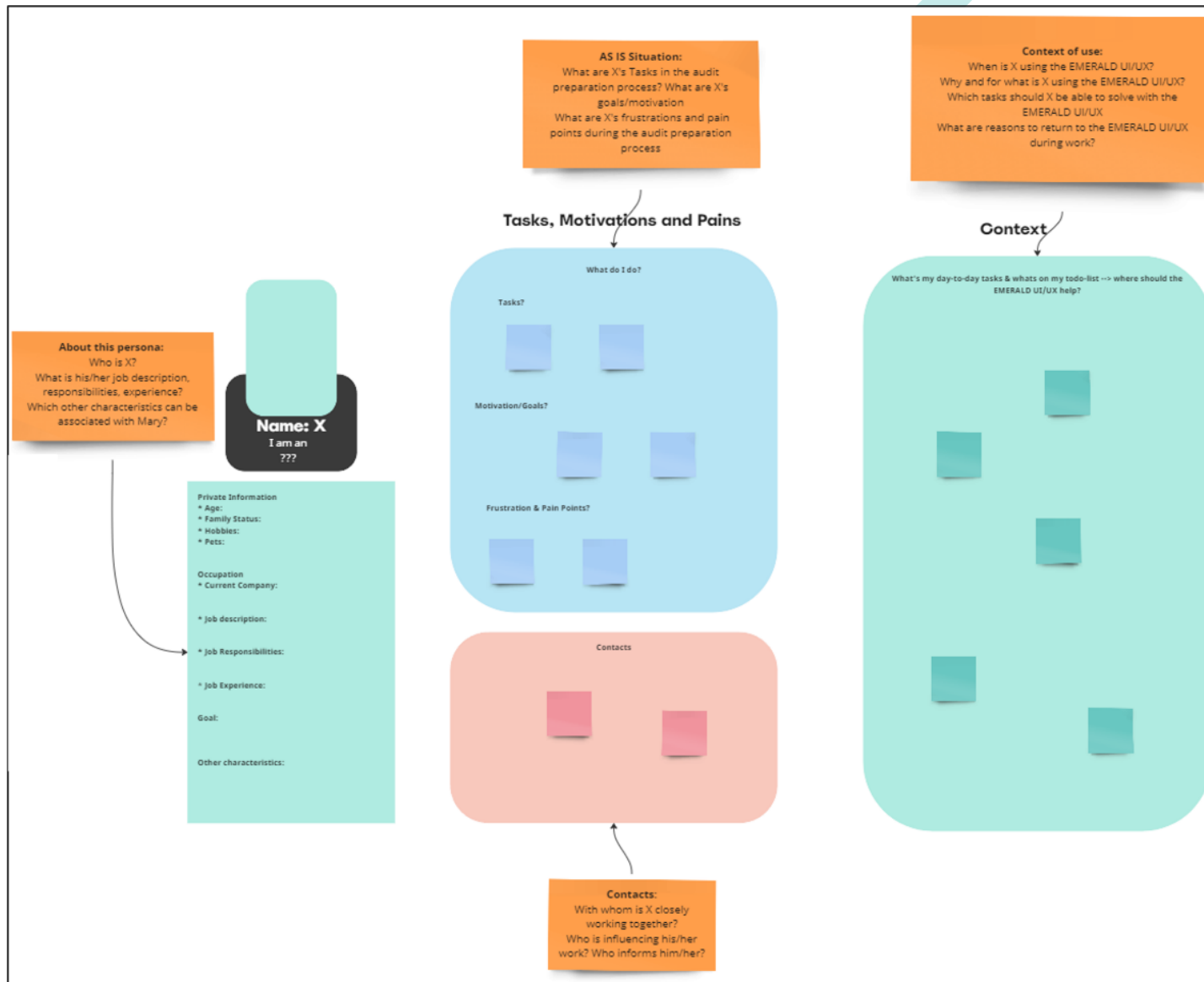


Figure 2. Persona Template

Workshop Part II: The second part of the workshop was attended by 9-11 participants. The agenda was as follows: first, we made a short recap of the first part of the workshop, by briefly summarizing the 4 personas developed. Second, we introduced scenarios and user stories as co-design method in general. Then we presented 6 pre-defined scenarios as starting point. 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. Thereby, 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 of how the persona would interact with the EMERALD UI and to discuss these user stories in relation to the pre-defined mock-ups.

Finally, 3 different scenarios were developed in this workshop (see Section 5.2):

- Scenario 1: Emerson – Bring your own certification scheme
- Scenario 2: Dylan – ICO Requirement Implementation
- Scenario 3: Charlie - Preparation of an audit by an internal auditor

2.4.2 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 [17], [18], [19]).

With regard to personas, there exist several strategies on how to mitigate gender bias during the development of personas and scenarios – one of them is to use gender-neutral personas (see [20], [21]) and to formulate scenarios in a gender-neutral way. Therefore, we created a list of gender-neutral names to use during the workshop, did not ask for a specific gender in the persona template, and afterwards, all gender specific formulations were removed (e.g., all wording referring to he/she were replaced with they).

To make the development of the personas more fun for the participants, we asked them to create a picture for each of the personas. However, as the resulting figures are not gender-neutral, they will be removed from the final version of the personas (in D4.2).

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; thereby, 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 manual process that is very time consuming and involves many people from different departments, as described in Table 3.

Table 3. Summary of answers given to the question Q1: “How do the current audit 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
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> multiple audits yearly time-consuming audits last 2-4 days significant preparation time manual preparation of procedures, policies, and documentation 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 4. 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 4. 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
<ul style="list-style-type: none"> costly processes (because of consultancy and manual work) large workload (because process is based on a spreadsheet which is then turned into tickets manually) 	<ul style="list-style-type: none"> audits comprehensive & time-consuming manual verification of extensive documentation involvement of multiple teams 	<ul style="list-style-type: none"> many people involved for a huge number of days for one single certification based on a spreadsheet 	<ul style="list-style-type: none"> 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 have concrete suggestions for specific tasks to be solved within the EMERALD project and especially by the EMERALD UI, as presented in Table 5. 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, including especially 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]!” (the spreadsheet is huge and used for managing all requirements of a respective standard).

Table 5. 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
<ul style="list-style-type: none"> automate collecting and identifying documentation (e.g., on employee certifications and trainings) facilitate and automate manual processes 	<ul style="list-style-type: none"> policy and procedure documentation management, integration of AMOE 	<ul style="list-style-type: none"> support the whole workflow management including a fair coverage of manual processes show path for new approach to audits 	<ul style="list-style-type: none"> 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

			<ul style="list-style-type: none"> • writing wrapper for tools to submit evidence • include on-premises assessment if desired • building internal tool similar to Clouditor² 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 6. 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 pilots, and iv) if possible, the solution developed within EMERALD should be accepted by auditors as a tool supporting the audit process.

Table 6. 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
<ul style="list-style-type: none"> • collect, identify and present important documentation • automate repetitive processes → reduce manual work 	<ul style="list-style-type: none"> • automate the verification process • main expectation: costs of the audits will be decreased 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 7. Nearly all partners use a spreadsheet to manage the requirements of the respective standards. One

² <https://github.com/clouditor/clouditor>

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 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 7. 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
<ul style="list-style-type: none"> • Spreadsheet • JIRA 	<ul style="list-style-type: none"> • Mostly manual • OpenStack • Spreadsheet/Word 	<ul style="list-style-type: none"> • Spreadsheet • Predefined Workflows and tickets • Internal monitoring tool 	<ul style="list-style-type: none"> • CIS benchmarks for cloud environments • Own centralized tool is planned with dashboard

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

Table 8 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 8. 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
<ul style="list-style-type: none"> • BSI C5 	<ul style="list-style-type: none"> • ISO • BSI C5 	<ul style="list-style-type: none"> • EUCS • BSI C5 • AIC4 	<ul style="list-style-type: none"> • ENS • DORA • Requirements from European Central Bank • Internal schemes

4 Work Processes

This section presents an overview of the work processes derived from the conducted interviews and focus groups. Firstly, we present the results of the interviews with the information security managers and compliance managers of the pilot partners, thus, we present the work processes and the individual steps they need to follow in order to thoroughly prepare an audit of cloud solutions. Secondly, we present the results of the interviews with the auditors. We show the work process and individual steps of how they conduct an audit for cloud solutions.

4.1 Work Processes of Compliance and Security Managers per Pilot

This section describes the results of the interviews and focus groups conducted with all pilot partners. Thereby, we present firstly the derived audit preparation processes, and secondly how EMERALD could be used to support these processes. The results presented are preliminary, as the conduction of the interviews and focus groups has not yet been finished. Additionally, all gained insights need to be discussed with the technical partners regarding their feasibility.

In the following, we present the work processes elicited from Pilot 2: CloudFerro, Pilot 3: Fabasoft and the processes derived for the compliance managers supported by NIXU. Please note that the work processes referring to IONOS and CaixaBank are omitted, as they are currently “work-in-progress”, and will be document in D4.2.

4.1.1 Pilot 2: CloudFerro

We conducted two interviews with CloudFerro employees: one with a compliance manager and one with a security manager. At the time of writing, the focus group is still pending, thus, we present here only the preliminary results that are up-to-change during the course of the project. In the following, we first present how the audit preparation processes take place at CloudFerro, as shown in Figure 3, and then how the EMERALD UI could support the different phases of the process, as shown in Figure 4.

- **Phase 1 – Starting with analysis:** In phase 1, the responsible person starts with a coordination check and gets in contact with the certification board. The audit preparation process differs a bit depending on if the audit preparation is done for a new certification scheme, for an existing certification scheme that was updated, or just checking the current certification scheme. If a new certification scheme is added, more work is needed to fulfil all requirements. If a certification scheme was updated, they check which requirements were updated and which are new, however, their goal is to implement as many of the requirements as possible in the most efficient way.
- **Phase 2 – Standard:** 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 requirements from the new standard, or only the new and updated requirements from the updated standard.
- **Phase 3 – Check with documentation:** All requirements 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 with the clarification of requirements.
- **Phase 4 – Identify gaps:** In this phase all existing gaps are identified to manage open requirements and discuss how to deal with them.

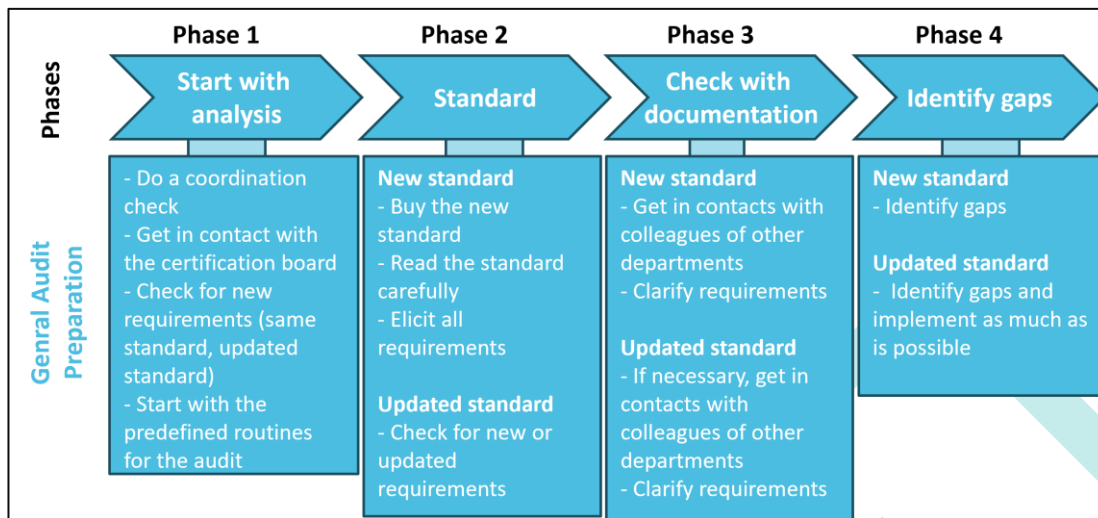


Figure 3. Individual phases of an audit preparation process of a compliance manager and security manager from CloudFerro

For three of the four phases mentioned above in the CloudFerro audit preparation process, 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 4 (in orange).

- Phase 2 – Standard:** EMERALD can support the compliance manager 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 requirements extracted from the new standard. Additionally, it can provide the possibility to add the corresponding metrics for each requirement.
 - **Update a Standard:** EMERALD can support the upload of an updated standard and allow audit instances to be updated with it. Additionally, the EMERALD UI shows updated requirements as well as new requirements that have been added to the updated version of the standard.
- Phase 3 – Check with documentation:** EMERALD can support the compliance manager 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 requirements.
- Phase 4 – Identify gaps:**
 - 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 requirements.

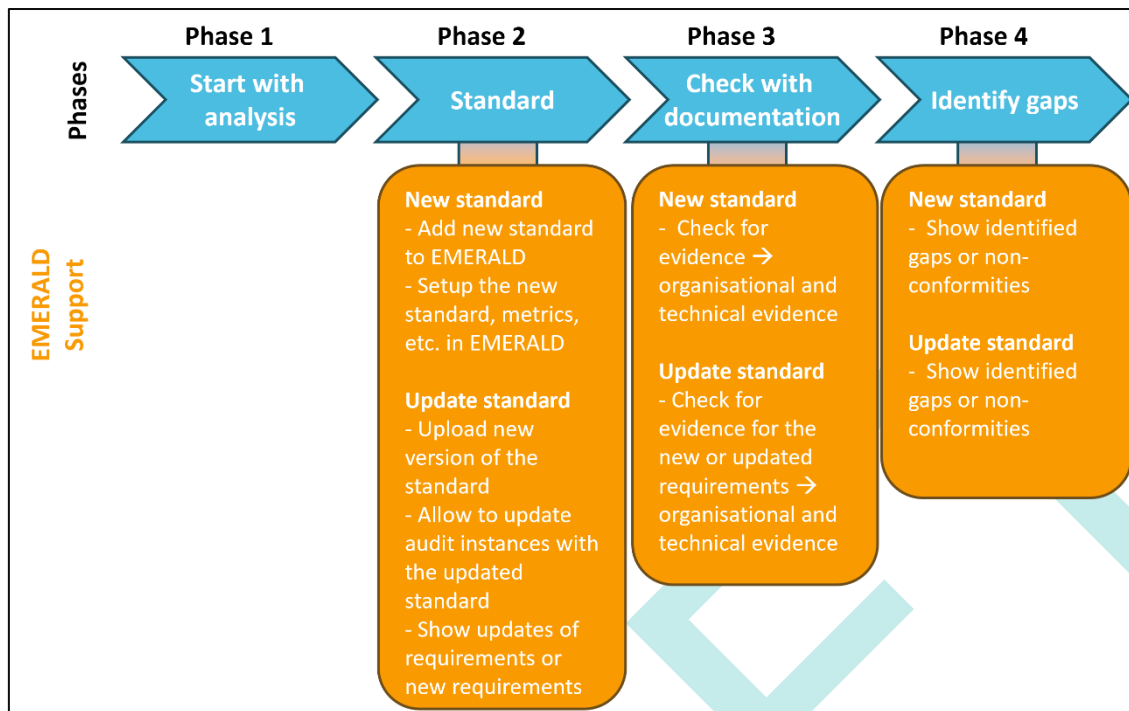


Figure 4. Potential support of the compliance manager and maybe security manager of CloudFerro during an audit preparation process with the EMERALD UI

4.1.2 Pilot 3: Fabasoft

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 to get input and feedback. Accordingly, we improved the elicited audit preparation process and present its actual status in Figure 5 as follows:

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

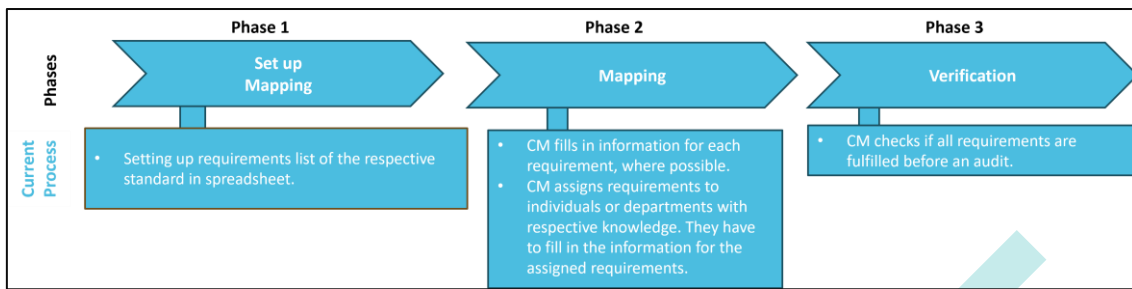


Figure 5. Individual phase of an audit preparation process of a compliance manager from Fabasoft

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 6 (in orange).

- Phase 1 – Set-up Mapping:** EMERALD can support the compliance manager with the following tasks for setting up the mapping:

 - Requirements overview: EMERALD UI can create a list with all requirements of the respective certification scheme for the upcoming audit.
 - Requirement parameters: EMERALD UI can provide the possibility to set the respective parameters for all requirements.
 - Requirement status: EMERALD UI can show the status of each requirement on two levels – compliance level and status level.
- Phase 2 – Set-up:** EMERALD can support the compliance manager with the following tasks:

 - Filtering: EMERALD UI allows to filter for requirements that need further input.
 - Add notes: EMERALD UI allows to add notes to a requirement e.g., suggestions on how a requirement can be addressed.
 - Assigning requirements: EMERALD UI allows to assign requirements to departments or individuals and vice versa, requirements can be assigned back to the compliance manager.
- Phase 3 – Verification:** EMERALD can support the compliance manager and the other departments with the following tasks during the verification phase:

 - Verification by departments or individuals: EMERALD UI allows the respective departments or individuals to verify the requirements and controls.
 - Verification by the compliance managers: EMERALD UI allows the compliance manager to mark the respective requirements as ready for being used in an audit.

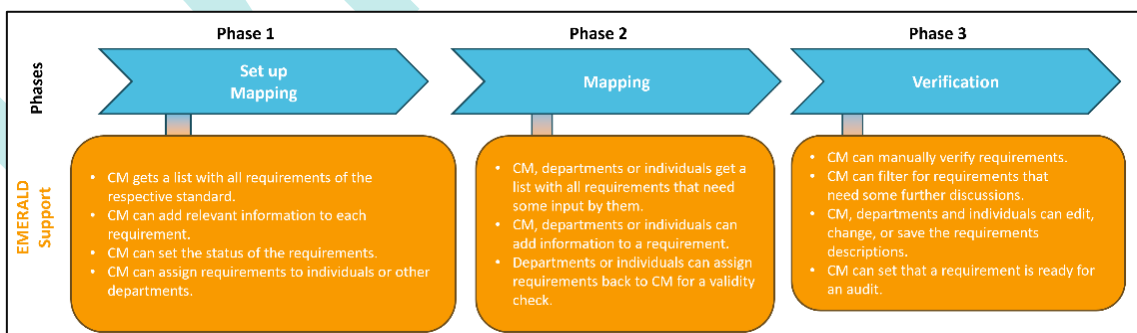


Figure 6. Possible support of the compliance manager of Fabasoft during an audit preparation process with the EMERALD UI

4.1.3 Compliance Manager from NIXU

An interview and a follow-up focus group was conducted with a compliance manager (not from NIXU) organized by the NIXU project manager. Again, we could derive the different process phases of how the audit preparation process is conducted, as depicted in Figure 7 (in blue), as follows:

- **Phase 1 - Preparation and Setup:** In this phase the whole audit preparation process is set up, including the establishment of the compliance framework, setting up the continuous compliance monitoring process, and informing all relevant stakeholders.
- **Phase 2 - Monitoring and Identification:** In this phase, the continuous monitoring and identification of the requirements 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:** 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:** If it has been decided to take corrective actions, these actions have to be planned, pursued, and implemented.
- **Phase 5 - Reporting:** In this phase all activities done regarding the requirements and their evidence, as well as all information related to corrective actions, need to be summarized in reports to be available for the audit itself.

For each of the five phases mentioned above in the audit preparation process, 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 7 (in orange).

- **Phase 1 - Preparation and Setup:** EMERALD can provide support for the following tasks:
 - Set-up: EMERALD UI can support the set-up of the respective compliance framework, standards, or certification schemes.
 - Cloud service: EMERALD UI can support the selection of the cloud solution to be audited.
 - Continuous monitoring setup: EMERALD UI can support to define specific parameters for the continuous monitoring of requirements and evidence.
 - Tasks & Meetings: EMERALD UI can offer to manage tasks or schedule respective meetings.
- **Phase 2 - Monitoring and Identification & Phase 3 - Evaluation & Decision Making:** EMERALD can provide support for the following tasks:
 - Continuous monitoring: EMERALD UI can help to support continuous monitoring of the system according to different parameters. Additionally, EMERALD UI should show possible deviations or non-conformities found in the corresponding visualisations in EMERALD UI.
 - Stakeholder involvement: EMERALD UI can help inform stakeholders when non-conformities, deviations or other problems occur (e.g., by automatically sending an email or displaying notifications).
- **Phase 4 - Corrective Action Planning & Implementation:** EMERALD can provide support for the following tasks:
 - Corrective Action Management: EMERALD UI should allow the possibility to note down decisions taken regarding the implementation of corrective actions. This includes, for example, having a list for 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 done within the EMERALD UI.
- **Phase 5 - Reporting:** EMERALD can provide support for the following tasks:
 - Requirements and Evidence: EMERALD could offer the possibility to create a document covering all information about the requirements and the respective evidence.
 - Support during audits: EMERALD could provide the possibility to download other types of reports to support the audit processes (e.g., different documents in different formats like Excel-Sheets, Word Files, etc.).

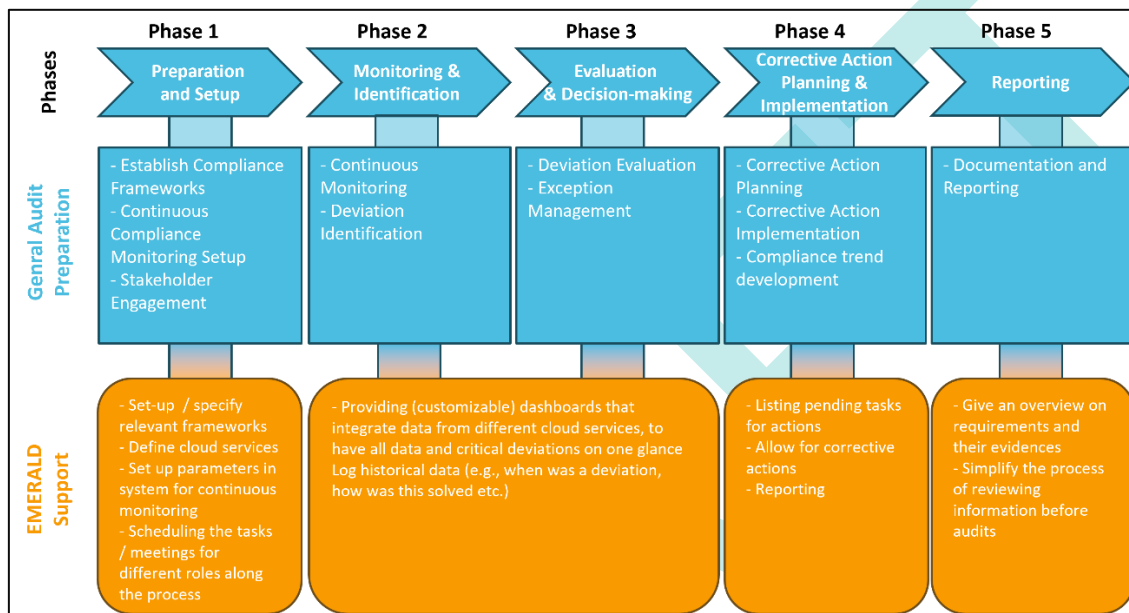


Figure 7. Individual phase of an audit preparation process of a compliance manager (blue) organized by NIXU and possible EMERALD support (orange)

4.2 Work Processes of Auditors

This section presents the results of an interview conducted with three auditors from NIXU. Based on the interview, we were able to derive the individual phases that auditors must conduct during an audit. Firstly, we present these phases and subsequently describe their enhancements for auditing cloud solutions, as depicted in Figure 8. Secondly, we present, for those phases where it is possible, how the EMERALD UI can provide the respective support.

We are aware that conducting an audit for cloud service providers is a very sensitive and challenging task that must ensure data protection throughout the entire process. Before conducting an audit, it is crucial to agree on the scope, limitations, and necessary details beforehand to differentiate the audit assessments from actual attacks by real adversaries. Additionally, it is essential to clarify that potential technical vulnerabilities should not be disclosed and that appropriate controls need to be established. Measures must also be taken to help defence and security teams to distinguish technical assessments conducted during the audit from genuine threats.

Keeping these security challenges in mind, an audit process consists of the following six phases:

- **Phase 1 – Initiating & Preparation:** 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 from the customer. This

documentation includes information about the technologies used, policies, configurations, and any other relevant details (see Figure 8, Phase 1 in blue).

Cloud solutions: Regarding cloud services this means to identify the respective cloud services being audited. Additionally, the documentation also includes information about the cloud solution (see Figure 8, Phase 1 in green).

- **Phase 2 – Audit Activities:** The audit activities consist of several steps (see Figure 8, Phase 2 – blue):

- 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.

Cloud solution: the document review includes documents about the cloud solution and its configurations (see Figure 8, Phase 2 – green).

- **Phase 3 – Technical Testing:** This phase involves specialized assessments performed by technical experts (see Figure 8, Phase 3 – blue). The testing includes:

- 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.

Cloud solution: specialists perform automatic and manual tests of the security, requirements and compliance of the cloud solutions (see Figure 8, Phase 3 – green).

- **Phase 4 – Reporting:** 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 (see Figure 8, Phase 4 – blue). 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:** 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 (see Figure 8, Phase 5 – blue).

- **Phase 6 – Certificate** (if applicable): Depending on the audit criteria and standards, if all requirements are met, the auditors may grant a certificate of compliance or conformance to the customer (see Figure 8, Phase 6 – blue).

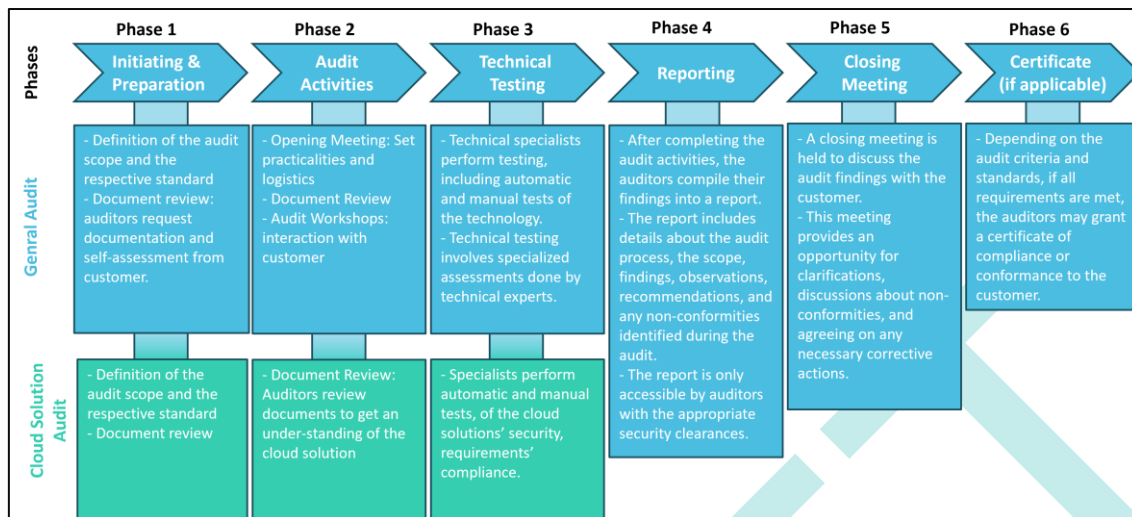


Figure 8. Individual phases for conducting audit processes of in general (blue) and enhanced for cloud solutions (green)

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/UX, as shown in Figure 9 (in orange):

- **Phase 1 – Initiating & Preparation:** EMERALD could support this phase as follows:
 - Audit scope: The audit scope determines the scope of the audit in relation to the respective standard to be audited and depends strongly on the customers' domain. EMERALD UI could offer a list of scopes tailored to the cloud solutions of the pilot partners.
 - Self-assessment questionnaire: The EMERALD UI can offer a self-assessment questionnaire for the pilots that allows them to self-assess their status regarding the fulfilment of the requirements with evidence. The EMERALD UI can support the export of the self-assessment questionnaire in form of a report that could be provided to the auditors.
- **Phase 2 – Audit Activities & Phase 3 – Technical Testing.** EMERALD could support both phases as follows:
 - Evidence: Show organisational evidence and technical evidence and their fulfilment regarding the standard and respective requirements.
 - Manual verification: Manual verification of requirements remains crucial for ensuring accuracy – this could be shown to the auditors.
 - Transparency: 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 requirements are validated. EMERALD UI should present an overview of the requirements 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:** EMERALD could support both phases as follows:
 - Audit report generation: EMERALD UI could offer the possibility to download all requirements 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.

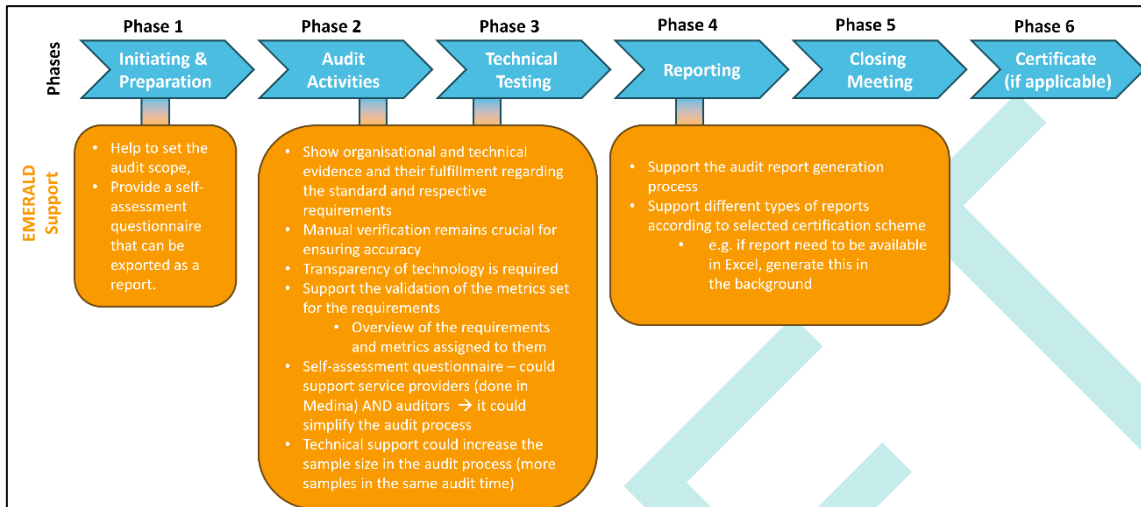


Figure 9. Possible support of the audit process with the EMERALD UI/UX

DRAFT

5 Personas & Scenarios

The first Personas & Scenarios workshop was divided into two parts, the first part to define personas and the second part to define scenarios for the respective personas. The methodology of the workshops is described in Section 2.4. The results of the workshop are described in the following sections – personas in Section 5.1 and scenarios in Section 5.2.

5.1 Personas

In the first part of the workshop, participants developed personas in smaller groups. Overall, four personas were developed: **2 different compliance manager personas, 1 internal control owner persona, and 1 auditor persona.** In the following, each persona is described in more detail.

5.1.1 Emerson - Compliance Manager in Financial Service Institution

The first persona – a compliance manager in a financial service institution – was named Emerson. The summarized persona is depicted in Figure 10.

- **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 provider, and assessing 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 that the management of 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 centralized point for evidence, metrics, and controls, further by automating tedious processes and management of numerous audits and thus minimizing human error and workload.

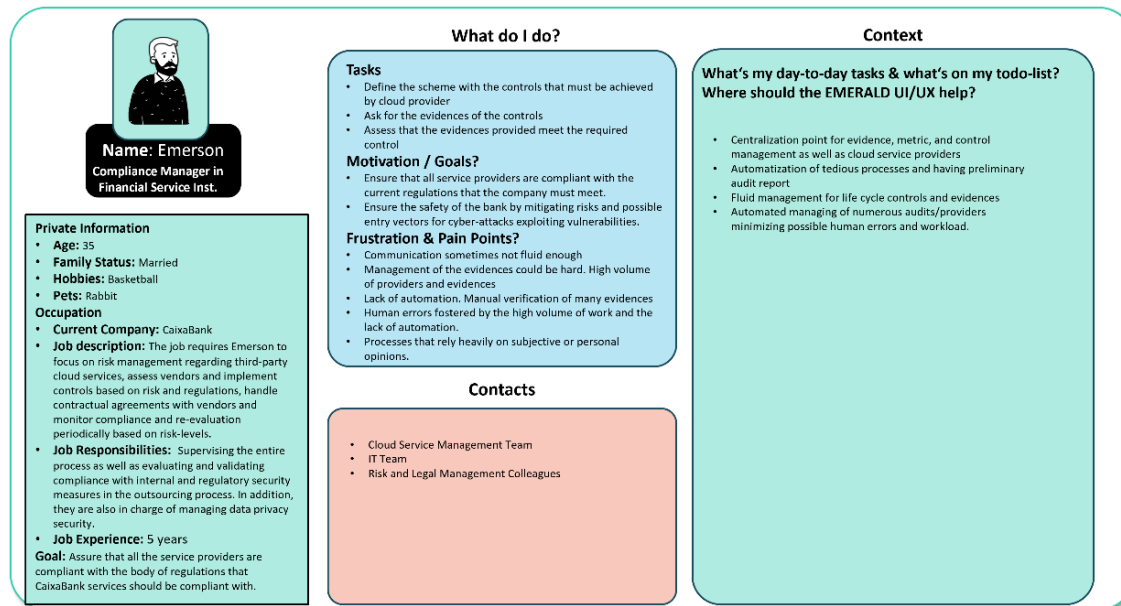


Figure 10. Persona Emerson – Compliance Manager in financial service institution

5.1.2 Riley – Cloud Service Compliance Manager

The second persona – a cloud provider compliance manager – was named Riley. The summarized persona is depicted in Figure 11.

- **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. Their 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 the day-to-day work.

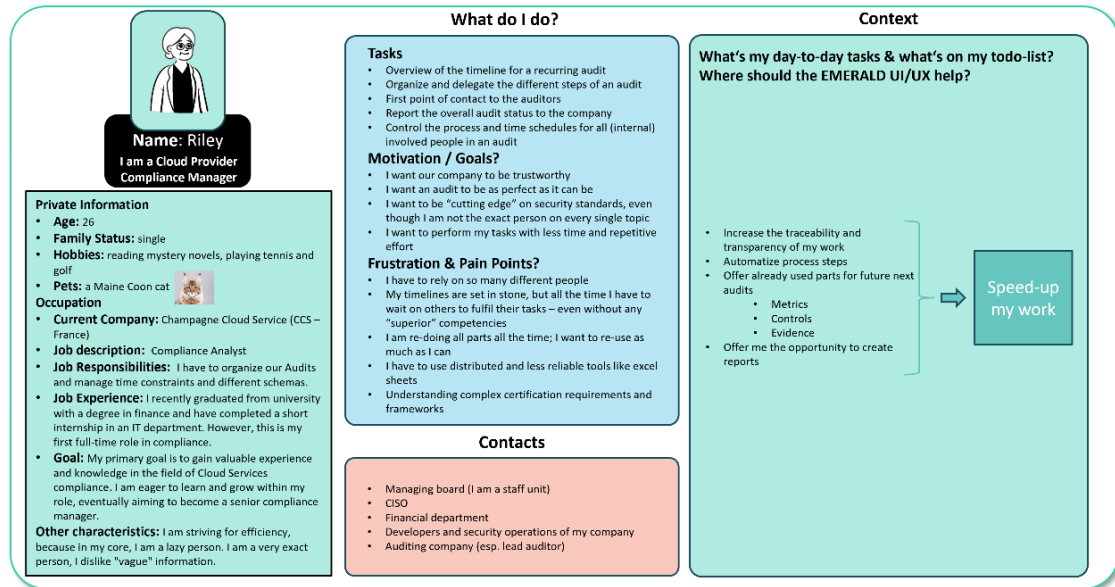


Figure 11. Persona Riley – Compliance Manager of a Cloud Provider

5.1.3 Dylan – Internal Control Owner

The third persona – an internal control owner – was named Dylan. The summarized persona is depicted Figure 12.

- **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 responsibilities are to ensure that requirements are addressed and that all evidence are 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.

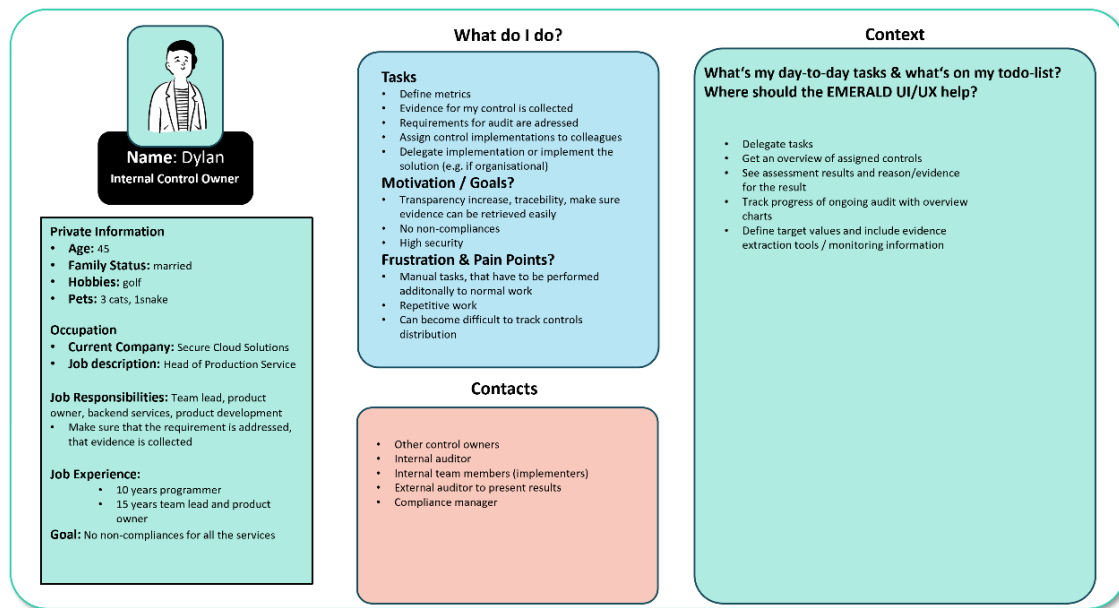


Figure 12. Persona Dylan – Internal Control Owner

5.1.4 Charlie - Auditor

The fourth persona – an auditor – was named Charlie. The summarized persona is depicted in Figure 13.

- **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 checks 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 generating reports on different levels of detail, for instance. With regard to evidence, Charlie would need to have access to a simplified evidence management system where it is possible to join evidence from different sources, for example. Additionally, EMERALD could help Charlie by integrating the automation of repetitive tasks, such as

the measurement of metrics, enabling information exchange with cloud service providers, and integrating external services, e.g., ticketing systems.

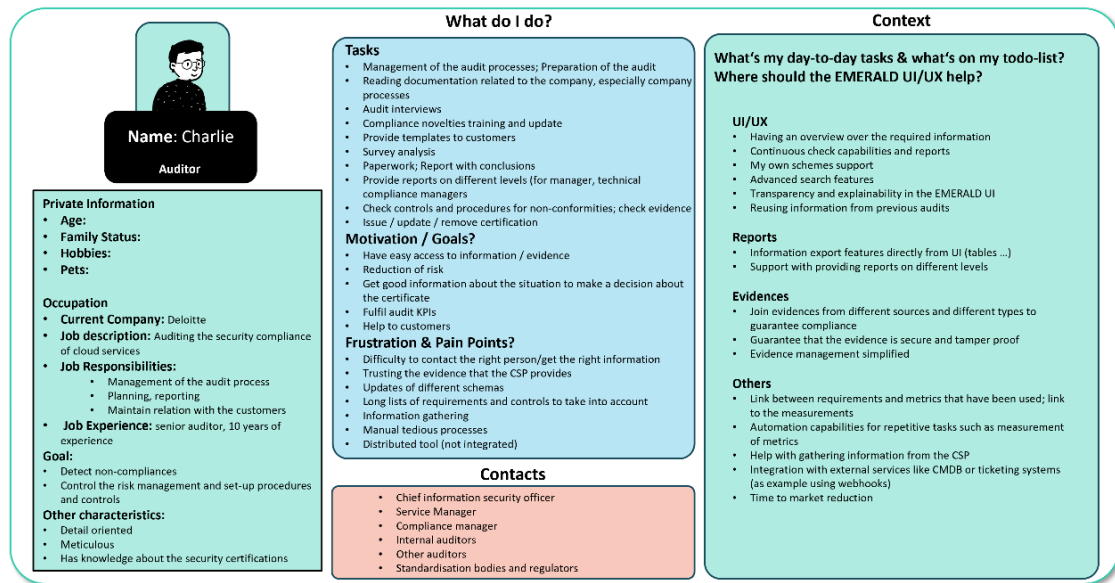


Figure 13. Persona Charlie - An (internal) auditor

5.2 Scenarios

In the second part of the Personas & Scenarios workshop, we asked the participants to develop scenarios using the previously developed personas as baseline (see Section 5.1). To do so, the participants selected predefined scenarios and used mock-ups (pre-created by WP4) to analyse how the tasks described in the scenarios could be performed with the user interface. We had predefined six general scenarios. Three of these scenarios were enhanced and adapted by the workshop participants to align them with the personas that were developed before. Thus, three detailed scenarios to understand the work of compliance managers in financial service institutions, internal control owners and auditors in more detail were created. Please note that scenarios were created for the personas Emerson, Dylan, and Charlie, and not for Riley due to the lower workshop attendance. However, Riley will be taken up in an upcoming workshop.

5.2.1 Scenario 1: Emerson – Bring Your Own Certification Scheme


The workshop participants adapted the scenario for the persona Emerson – a compliance manager in a financial service institution – to fit the persona's tasks. The short scenario description is presented below and the whole scenario is depicted in Figure 14.

Generally, in this scenario, Emerson's goal would be to define its own certification scheme, thus, the new certification scheme should be a selection and combination of requirements from other certification schemes ("Bring Your Own Certification Scheme - BYOCS" option). 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 instance (=target of evaluation) to manage cloud solutions and the corresponding BYOCS. Emerson opens EMERALD, selects the audit instance 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 requirements and controls, for which Emerson goes to the EMERALD UI. Emerson uses different EMERALD UI functionalities to filter the

requirements and uses different visualizations of the overall status of all requirements to determine which requirements need to be dealt with and which are already compliant.

EMERSON – Bring your own certification schema.

- 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 requirements 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 requirements.
- Emerson's task is now to go through all requirements and 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 requirements regarding the controls, evidences and status.
- Emerson uses different functionalities available in the EMERALD UI to filter requirements and uses different visualisations of the overall status of all requirements, etc., to find out which requirements need some treatment, and which are already ok.



Name: Emerson
Compliance Manager in
Financial Service Inst.

Figure 14. Scenario 1: Emerson – Bring your own certification scheme


5.2.2 Scenario 2: Dylan – Internal Control Owner Requirement Implementation

The workshop participants developed a scenario for the persona Dylan – an internal control owner (ICO) – that corresponds with Dylan's working tasks. The scenario is shortly summarized below, and the detailed description is depicted in Figure 15.

Overall, in this scenario Dylan opens the EMERALD UI, assesses a requirement/control that is still open and would like to delegate the implementation of this control to a colleague Y. Y selects a set of metrics that matches the requirement, implements the requirement and informs Dylan via the EMERALD UI that the metric was implemented. Dylan checks whether the metric has been implemented correctly and meets the requirements.

DYLAN – ICO Requirement 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 of controls (metrics?) and for tracking the progress of the implementation.
- Dylan opens the EMERALD UI, opens the respective requirement and wants to distribute the implementation of a control to their colleague Y.
- Y chooses a set of metrics that fit the requirement.
- Y implements the requirement and sends it back to Dylan.
- Dylan checks that the requirement is correctly implemented and compliant



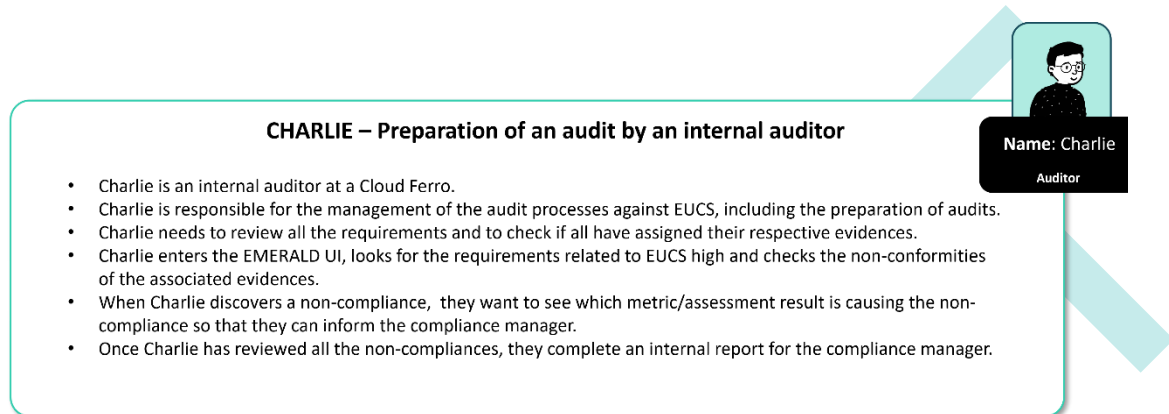
Name: Dylan
Internal Control Owner

Figure 15. Scenario 2: Dylan – Internal Control Owner Requirement Implementation

5.2.3 Scenario 3: Charlie – Preparation of an Audit by an Internal Auditor

The scenario for the persona Charlie - an auditor - was adapted from a pre-defined one to be in line with the auditors' tasks. A short description is provided below, and the detailed scenario is shown in Figure 16.

In this scenario, Charlie would like to review all requirements according to their compliance status. Charlie enters the EMERALD UI, looks for the requirements related to EUCS high and looks for requirements which are marked as non-compliant. Charlie has a closer look to 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.



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 requirements and to check if all have assigned their respective evidences.
- Charlie enters the EMERALD UI, looks for the requirements 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
Auditor

Figure 16. Scenario 3: Charlie - Preparation of an audit by an internal auditor

DRAFT

6 UI/UX Requirements (version 1)

In every software project it is extremely important to document requirements to ensure that the desired functionalities are implemented and validated. In the case of the EMERALD UI/UX, the requirements define which elements should be presented to the user, how they interact with each other, and the EMERALD architecture.

Overall, three different types of requirements are elicited in EMERALD. In WP1, all technical requirements for the different EMERALD components are collected and will be summarized in D1.3 “EMERALD solution architecture-v1”. In WP5, business-driven requirements from the pilots are elicited and presented in D5.1 [22]. In WP4, requirements for the EMERALD UI – the graphical user interface (GUI) - are elicited and are presented in this deliverable.

So far, we have elicited 17 requirements for the EMERALD UI (GUI) by analysing the interviews and focus groups conducted with the pilot partners. We homogenized the requirements based on their similarities and added them to the common Git repository of the EMERALD project.

Each requirement is presented along the common EMERALD requirement definition table consisting of the following fields:

- **Requirement id:** Contains the unique identifier for the requirement. All requirements referring to the EMERALD UI begin with “UIUX” followed by a unique number e.g., UIUX.01.
- **Short title:** Contains a short title for the requirement.
- **Description:** Describes the requirement in more detail.
- **Status:** Contains the status of the requirement, consisting of one of the following values: Proposed → Accepted/Discarded → Work in Progress → Implemented (Partial/Full) → Tested → Validated
- **Priority:** Priority values are: Must; Should; Could.
- **Component:** Contains the name of the component the requirement is related to; in the case of WP4 it is “EmeraldUI”.
- **Source:** Defines where the requirement comes from: pilot, component, DoA or KPI.
- **Type:** Describes the type of the requirement. In the case of WP4 it is always a “GUI” requirement.
- **Related KR:** Describes the related key result of the DoA. In the case of WP4, the related key result is “KR6_EMERALD_UI/UX” (see below).
- **Related KPI:** Describes the related key performance indicator of the DoA. So far, all requirements refer to KPI 6.3 (see below).
- **Validation acceptance criteria:** Describe how to validate the requirement.

The related key result for all the UI/UX requirements is:

- **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 [1].

Currently, the requirements are related to KPI 6.3:

- **KPI 6.3:** Provide a graphical user interface for role-based access to certification information content [1].

The following tables present the collected requirements for developing the EMERALD UI/UX. Please note that the requirements collected so far are an initial set of requirements that will be enhanced, reworked and improved in the coming months. The final set of the UI/UX Requirements will be presented in D4.2 (M18).

Landing Page

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: <ul style="list-style-type: none"> • Audit Instance Creation View • MARI Tool View • Certification Schemes Manager View
Status	Proposed
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.

Audit Instance Creation View

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: <ul style="list-style-type: none"> • 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 <p>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.</p>
Status	Proposed
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.
--------------------------------	--

Requirements Overview View

Field	Description
Requirement id	UIUX.03
Short title	Requirements Overview View
Description	<p>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:</p> <ul style="list-style-type: none"> • ID • Description • Owner • Person or department to whom the requirement is currently assigned • Compliance • Status <p>Compliance can be one of:</p> <ul style="list-style-type: none"> • Compliant • Non-compliant <p>Status can be one of:</p> <ul style="list-style-type: none"> • Open • Need for discussion • Waiting for input • Waiting for confirmation by CM • Verified
Status	Proposed
Priority	Must
Component	EmeraldUI, RCM, Cloudditor-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.

Requirements Overview View: Progress Indicators

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	Proposed
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.
--------------------------------	--

Requirements Overview View: Filtering and Searching

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	Proposed
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.

Policy Documents Manager View

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	Proposed
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.

Policy Documents Manager View: Metrics Selection

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	Proposed
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.
--------------------------------	---

Evidence Extractors View

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	Proposed
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.

Requirement Detail View

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	Proposed
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.

Requirement Detail View: Assignment

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	Proposed
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.

Requirement Detail View: History

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	Proposed
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.

Requirement Detail View: Evidence

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	Proposed
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.

Requirement Detail View: Non-Compliance

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	Proposed
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.
--------------------------------	--

MARI Tool View

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	Proposed
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.

Certification Schemes Manager View

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	Proposed
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.

Certification Schemes Manager View: BYOCS

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	Proposed
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.
--------------------------------	--

Certification Schemes Manager View: Import/Export

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	Proposed
Priority	Could
Component	EmeraldUI, Cloudfitor-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.

DRAFT

7 Conclusions

This deliverable has presented the overall methodology used in WP4 and the first results achieved by applying different methods in the context of the EMERALD project. In more detail:

- From the interactive interview session conducted at the Bilbao general assembly, we were able to derive insights about the **pilots' audit preparation processes** in general, their **needs**, some **pain points** and **expectations** towards EMERALD.
- From the interviews and focus groups, we were able to **derive concrete initial work processes** per pilot and for auditors in relation to preparing and conducting audits from the perspective of compliance managers, security managers and auditors.
- From the Personas and Scenarios workshop, we derived four personas – **2 different compliance manager personas**, **1 internal control owner persona**, and **1 auditor persona**. Additionally, we developed **6 general scenarios** and **3 detailed scenarios** to understand the work of compliance managers, internal control owners and auditors in more detail.
- Finally, we were able to derive **17 UI/UX requirements** for developing the EMERALD UI/UX.

As all results presented in this deliverable are work in progress, we will continue working on them until M18. In more detail:

- We will continue with interviews and focus groups to get a more detailed overview of all work processes of all pilots and auditors.
- From all work processes we plan to derive a condensed work process that combines the insights gained from the individual work processes of each pilot partner.
- We will continue with the development of the derived personas and create so-called “personas-to-go”, and will deepen the scenarios so that they can be related to the envisaged EMERALD UI/UX. This is also necessary to develop the envisioned interaction concept.
- Finally, we will enhance our initial set of UI/UX requirements that will be subsequently used to realise and implement the EMERALD UI/UX.

This document is the first version of the results of the UI-UX requirements analysis and the work processes for the EMERALD UI/UX, where we established the overall methodological approach of our work. In M18 of the EMERALD project, we will provide an updated version of this document with in-depth work processes and a final set of the requirements for the UI/UX - D4.2 – Results of the UI-UX requirements analysis and the work processes – v2 (M18).

8 References

- [1] EMERALD Consortium, “EMERALD - Annex 1 - Description of Action - GA 101120688,” 2022.
- [2] EMERALD Consortium, “Home page,” [Online]. Available: <https://www.emerald-he.eu/>. [Accessed June 2024].
- [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. Fessler, V. Pammer-Schindler, K. Pata, S. Feyertag, M. Möttus, 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. Grønbaek, “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, “D7.2 Data Management Plan–v1,” 2024.
- [9] J. Gläser and G. Laudel, *Experteninterviews und qualitative Inhaltsanalyse*, Springer-Verlag, 2010.
- [10] D. L. Morgan, “Focus Groups,” *Annual Review of Sociology*, vol. 22, pp. 129-152, 1996.
- [11] A. Cooper, “The Inmates are Running the Asylum,” in *Software-Ergonomie '99: Design von Informationswelten*, Wiesbaden, Vieweg+Teubner Verlag, 1999, pp. 17-17.
- [12] T. Adlin and J. Pruitt, *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*, Elsevier, 2006.
- [13] P. Turner and S. Turner, “Is stereotyping inevitable when designing with personas?,” *Design Studies*, vol. 32, no. 1, pp. 30-44, 2011.
- [14] 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.
- [15] A. Cooper, R. Reimann, D. Cronin and C. Noessel, *About Face: The Essentials of Interaction Design*, John Wiley & Sons, 2014.

- [16] 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.
- [17] C. Ashcraft, B. McLain and E. Eger, “Women in tech: The facts,” National Center for Women & Technology, 2016.
- [18] J. E. Fountain, “Constructing the information society: women, information technology, and design,” *Technology in Society*, vol. 22, no. 1, pp. 45-62, 2000.
- [19] J. Wajcman, “Reflections on Gender and Technology Studies,” *Social Studies of Science*, vol. 30, pp. 447-464, 2000.
- [20] 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.
- [21] 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.
- [22] EMERALD Consortium, “D5.1 Pilot definition, set-up & validation plan,” 2024.
- [23] 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 Fessler. I am

EMERALD is an HEU Project (GA no.: 101120688) with the objective to pave the road towards Certification-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 cloud 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]?
 - o 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]?
 - o What would be helpful for you in general?
 - o What could be useful features?
 - o Which information / data should such a tool provide for your work?
 - o 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]?
 - o 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 EU 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 slideset 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.” [23]

- What do you associate with the term AI / artificial intelligence?
 - o 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 Certification-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 Fessler, Know-Center GmbH, afessler@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 Certification-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:	<p>You have the right to:</p> <ul style="list-style-type: none"> - 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 <p>To exercise these rights please contact datenschutz@know-center.at</p> <p>You also have a right to make a complaint to the Data Protection Authority.</p> <p>In this regard, we also refer to their homepage, which can be accessed under the link https://www.dsb.gv.at</p>