Deliverable D4.4

User interaction and user experience concept – v2

Editor(s):	Angela Fessl, Katharina Stefan
Responsible Partner:	Know Center Research GmbH
Status-Version:	Final – v1.0
Date:	31.10.2025
Type:	R
Distribution level (SEN, PU):	PU

Project Number:	101120688
Project Title:	EMERALD

Title of Deliverable:	D4.4 User interaction and user experience concept – v2
Due Date of Delivery to the EC	31.10.2025

Workpackage responsible for the Deliverable:	WP4 - User interaction and user experience development
Editor(s):	Angela Fessl, Katharina Stefan (KNOW)
Contributor(s):	Christian Banse (FHG) Franz Deimling, Björn Fanta (FABA) Marinella Petrocchi (CNR) Juncal Alonso, Cristina Martínez, Iñaki Etxaniz Errazkin (TECNALIA)
Reviewer(s):	Mika Leskinen (DNV/NIXU) Cristina Martínez, Juncal Alonso (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	WP1, WP2, WP3, WP5, WP6

Abstract:	Final version of the report on the developed mock-ups for the user interaction and user experience concept
Keyword List:	Paper-based mock-ups, final clickable mock-ups, final user journeys
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	03.10.2025	First draft version	Angela Fessl, Katharina Stefan (KNOW)
v0.2	12.10.2025	QA review. Some modifications proposed by the reviewer	Mika Leskinen (DNV/NIXU)
v0.3	14.10.2025	Integration of the feedback received from QA review	Angela Fessl (KNOW)
v0.4	15.10.2025	D4.4 sent to Tecnalia for final review	Angela Fessl (KNOW)
v0.5	17.10.2025	Final QA review	Cristina Martínez, Juncal Alonso (TECNALIA)
v0.6	28.10.2025	Integration of the feedback received from final QA review	Angela Fessl, Katharina Stefan (KNOW)
v1.0	31.10.2025	Submitted to the European Commission	Cristina Martínez, Juncal Alonso (TECNALIA)

Table of contents

List of tables

List of figures

Terms and abbreviations

AI-SEC	AI Security Evidence Collector
AMOE	Assessment and Management of Organisational Evidence
BYOCS	Bring Your Own Certification Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik
CaaS	Certification-as-a-service
CISO	Chief Information Security Officers
CM	Compliance Manager
CSP	Cloud Service Provider
DoA	Description of Action
EAB	External Advisory Board
EC	European Commission
ECM	Expert Compliance Manager
ENS	Esquema Nacional de Seguridad
EUCS	European Cybersecurity Certification Scheme for Cloud Service
GA	Grant Agreement to the project
ICO	Internal Control Owner
KPI	Key Performance Indicator
MARI	Mapping Assistant for Regulations with Intelligence
M	Mean Value
NLP	Natural Language Processing
OSCAL	Open Security Controls Assessment Language
RCM	Repository of controls and metrics
SD	Standard deviation
SUS	System Usability Score
TLS	Transport Layer Security
ToE	Target of Evaluation
TWS	Trustworthiness System
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 the vision of Compliance-as-a-service (CaaS) and its continuous and lean re-certification aspects with a focus on the pilot partners and component owner's needs. The goal of compliance-as-a-service is to develop an integrated, easy to use, and fully-fledged UI/UX for the EMERALD solution.

This deliverable D4.4 is related to *WP4 - User interaction and user experience development* and presents the final results regarding *T4.3 - Designing a user interaction and user experience concept.* The document describes the applied methodology for deriving the user interaction concept and the user interface by considering the needs from the pilot partners as well as the component owners. The deliverable also presents two sets of paper-based mock-ups of the EMERALD UI/UX that were developed and presented in D4.3 [1], and the final version of the clickable mock-ups.

In more detail, this deliverable presents the following results:

- **Methodology**: The whole co-creation and co-design approach used for developing the EMERALD UI/UX. The methodology used brought together the needs of the pilot partners and the available EMERALD components including the features and functionality from the technological component owners.
- **The final user journeys**: Based on the different workshops, we present the final user journeys aligned with the developed personas and scenarios.
- **Clickable mock-ups**: We present the final workflow for the EMERAD UI. Additionally, we present the final version of the **clickable mock-ups** for **the integrated EMERALD UI**.
- **Validation**: We present the results of a UI Validation of the clickable mock-ups by the consortium partners as well as the insights we received from the EMERALD Expert Advisory Board.

This deliverable concludes the work done in *T4.3 - Designing a user interaction and user experience concept* (M24). The clickable mock-ups serve as guideline for implementing the EMERALD UI in *T4.4 - Technical implementation of EMERALD UI*.

1 Introduction

The EMERALD UI/UX offers the user interface (UI) and user experience (UX) to address compliance-as-a-service (CaaS) and its continuous and lean re-certification aspects with a focus on the user's needs. The user experience (UX) is the overall experience a user has when interacting with a product, focusing on understanding their needs, behaviours, and pain points. It aims to design intuitive, efficient, and satisfying experiences through factors like usability, accessibility, information architecture, and interaction design. The UI, on the other hand, deals with the visual and interactive aspects of a product, such as layout, typography, buttons, and colour schemes. Its goal is to create an appealing and easy-to-navigate interface, helping users quickly find what they need and complete tasks efficiently.

In this deliverable, we present the final version of the clickable mock-ups for the integrated EMERALD UI/UX. Different methods were applied and different activities and workshops were conducted bringing together the insights gained from the EMERALD pilot partners and the EMERALD component owners. The goal of the EMERALD UI is to provide the EMERALD target users a seamless user experience for continuous auditing in the cloud cybersecurity domain, offering easy-to-use and explainable workflows to support the auditors' work and the audits conducted.

This section sets this deliverable into the context of the overall EMERALD project, presents the goal of the deliverable, as well as the target audience and the document structure. It also summarizes the final results of task *T4.3 - Designing a user interaction and user experience concept.*

1.1 About this deliverable

This deliverable is related to the project's key results (KR6), defined in the DoA [2] as:

"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."*

This deliverable summarizes the final results tailored to reach key result KR6 of the project. It presents the methodological approach taken to develop an integrated user interface for EMERALD and presents the final concrete outcomes regarding *T4.3 - Designing a user interaction and user experience concept*. These outcomes consist of paper-based and the final clickable mock-ups on how the EMERALD UI/UX should look, covering the perspectives of the pilot partners as well as the component owners of EMERALD.

Different methods have been used and applied for developing the EMERALD UI, consisting of three major iterative approaches and following a co-design, participatory, and contextual design approach:

- **Interviews with the pilot partners**: A series of interviews and focus groups with the pilot partners was conducted to derive insights about the working processes and tasks in the respective companies. From the insights gained, a first set of paper-based mock-ups was developed.
- **Development of personas, scenarios and user journeys**: Different workshops with project partners were conducted for developing personas, scenarios, and user journeys. Especially the user journeys were used for developing concrete interactions of a

respective persona with the EMERALD UI to fulfil specific tasks. The insights from the user journeys helped to improve the paper-based mock-ups.

- **Individual workshops with the component owners:** Different workshops were conducted with the individual EMERALD component owners to investigate which information the different components offer and how to integrate them into the EMERALD user interface. The paper-based mock-ups were used as a baseline, and after having discussed them, the clickable mock-ups of the EMERALD UI were developed.
- **Further workshops:** To continuously improve the EMERALD UI, further workshops were held with the pilot partners and technical component owners. Our goal was to elicit all necessary and relevant information from all stakeholders involved to gather their feedback and new insights, to clarify misunderstandings, and allow their input to be integrated throughout the whole design phase.

The target audience of this deliverable is twofold:

- First, all EMERALD partners: The pilot partners, as their employees including compliance managers, internal control owners and auditors, are the target groups of the EMERALD project. The technical partners, because their components and the corresponding outputs will be connected to and presented in the EMERALD UI.
- 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, workshops) and derive mock-ups that are iteratively refined with the target users. It shows how to carry out a user interface development process that corresponds to the needs and wishes of the target users.

The goal of this deliverable is to present the applied methodology as well as the final version of the clickable mock-ups for the EMERALD UI.

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 4.3, and includes separate sub-sections for each step of the methodology taken to describe the different phases of the development of the EMERALD UI/UX.

The subsequent sections –Section 3, Section 4, and Section 5 - present the achieved results in detail. Section 3 presents a short summary of the final set of personas and scenarios, followed by a detailed description of the developed user journeys, including the interaction of the personas with an EMERALD UI. As a starting point for developing the clickable mock-ups, a set of paper-based mock-ups were developed; these have not been further refined because with the change to Figma all relevant mock-ups were added there; therefore the paper-based mock-ups are presented in *APPENDIX A: Mock-ups derived from Interviews with Pilot Partners*, *APPENDIX B: Mock-ups derived from the interviews,* and *APPENDIX C: User Journeys and paper-based* Mock-ups. Section 4 presents a summary of the clickable mock-ups along a workflow process covering all relevant features of the EMERALD solution. Additionally, we present the user rights along the personas developed. Section 5 presents some first validation results gained from the EMERALD consortium as well as feedback received from the External Advisory Board (EAB).

Finally, Section 6 concludes the report with the major results achieved in T4.3.

The results presented in D4.3 [1] regarding the paper-based mock-ups that were derived from the interviews and focus groups conducted with the pilot partners and which served as starting point are included for completeness sake in *APPENDIX A: Mock-ups derived from Interviews with Pilot Partners*, *APPENDIX B: Mock-ups derived from the interviews*, and *APPENDIX C: User Journeys and paper-based* Mock-ups.

1.3 Technological Advances from the MEDINA project

The EMERALD project builds on the foundations of the earlier MEDINA project: *Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme* (GA 952633) [3], a Horizon 2020 research and innovation action. In MEDINA, a range of technical components were developed, but they largely operated as standalone tools. Most had individual user interfaces, yet there was no unified framework to bring them together.

EMERALD advances this work by pursuing one of its central objectives: the creation of an integrated user interface (UI). This UI consolidates the MEDINA components—further enhanced within EMERALD—into a single, coherent compliance-as-a-service framework. Crucially, the EMERALD UI is not designed in isolation. It is tailored to the needs of all pilot partners through a co-design and co-creation process, ensuring usability and practical relevance. Unlike MEDINA, where such participatory design was not foreseen, this approach has significantly strengthened EMERALD's outcomes, delivering a more user-centred and impactful solution.

1.4 Updates from D4.3

This deliverable evolves from D4.3 [1]. Our ultimate goal is to make this deliverable self-contained. Therefore, several sections that have not been changed have been directly taken over from D4.3. Other parts that have been developed during the last year are new. To simplify the tracking progress and updates from the previous version, Table 1 briefly summarises the changes and additions to each section of the document.

Table 1. Overview of Deliverable Updates with respect to D4.3

Section	Changes
1. Introduction	It is based on the text from D4.3 but enhanced with the new achievements and results.
2. Methodology	This section was updated; all further activities that have taken place between M12 and M24 of the project have been added.
3. User Journeys	This section was updated and restructured; reworked and improved user journeys were added there. The originally developed paper-based mock-ups have been moved to the Appendixes to make this section clearer.
4. Clickable Mock-up	This section was completely updated and covers a detailed description of the developed UX workflows and most of the screens of the clickable mock-up.
5. Validation	This section is new and presents first insights from some UI testing with EMERALD's target users and feedback from the EAB.

2 Methodology

The overall methodology of WP4 follows a co-design, participatory and contextual design approach (see [4], [5], [6], and [7]) using different methods such as interviews, workshops, and mock-ups development. A co-design strategy like this seeks to close the communication gap between target users, technology developers, and designers. This method, which came forth as a result of designers and end users working together, moved the emphasis from just making things to taking care of users' requirements [7]. Similar ideas are emphasized by terms like "co-design", "participatory design" and "contextual design", which emphasize the active participation of all stakeholders to satisfy organizational and individual goals [8], in accordance with software developers. Giving end users a voice during the development of the software they will use can be seen as an empowering act [7]. Co-creation involves shared creativity [6], while co-design applies this creativity throughout the entire design process [6]. Throughout the whole development process, active user participation is encouraged, creating a hybrid space that combines users' and developers' knowledge and feedback. This shift from "user as subject" to "user as partner" has changed stakeholder roles [6], with users potentially becoming meta-designers and researchers acting as facilitators. Co-design is characterized by iterative learning processes involving all relevant stakeholders. In EMERALD's case the stakeholders consist of the pilot partners, and an external auditor company (DNV/NIXU) (as end users), the component owners (as software developers), as well as the members of the External Advisory Board (EAB).

Mock-ups were used in industrial design long before they were used in software design processes [9]. In the middle of 1990s, a number of well-known companies adopted paper prototyping in their product development process [10]. Prototypes were already taken into consideration by Floyd [11] as a way to help software developers and customers communicate and provide feedback, and by Ehn [12], who regarded prototypes as a way to help designers as well as a way to involve non-experts in the design process. According to Bødker and Grønbaek [8], the goal of cooperative prototyping is to start a design process where users and designers actively and creatively work together to create a prototype, with the goal of giving users the chance to experiment with it and to try it out.

In software development, mock-ups and clickable prototypes are essential tools that facilitate the visualization and testing of a product before full-scale development [10]. Mock-ups are static representations of a user interface, providing a detailed visual design without interactive elements. They help stakeholders and developers understand the look and feel of the final product. Clickable prototypes, on the other hand, are interactive models that simulate the user experience by allowing users to click through the interface as they would in the final product [13]. These prototypes are crucial for usability testing, enabling early detection and resolution of potential issues. Utilizing these tools not only improves communication among team members but also accelerates the development process by providing clear guidance and reducing the need for extensive revisions.

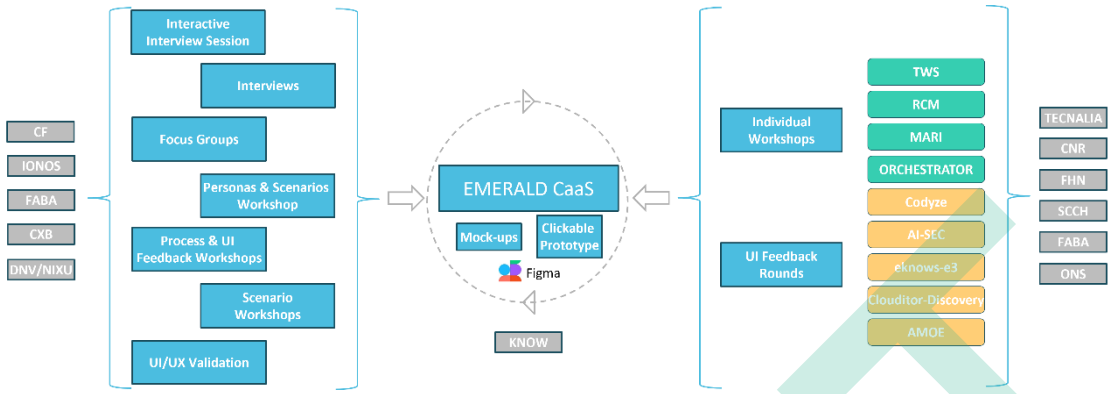

Figure 1. Overall Methodology for developing the EMERALD UI.

The application of co-design as the overarching technique for WP4 activities was viewed as a feasible way to close the gap between the EMERALD pilot partners and technology partners in order to create an advanced EMERALD UI/UX that satisfies their respective needs. The overall goal is to have a fully developed user interaction and user experience concept that can be validated regarding its usefulness and acceptance together with the target groups.

Figure 1 presents the methodology applied for developing the EMERALD UI so far. The first mock-ups were developed with the insights gained from the pilot partners – the EMERALD target users. These mock-ups were then iteratively refined with the component partners – the EMERALD technology partners. In more detail:

- **Pilot partners**: In spring 2024, we conducted a series of interviews with the pilot partners (see D4.2 [14]). From these interviews, a first set of paper-based mock-ups were developed (see *APPENDIX A: Mock-ups derived from Interviews with Pilot Partners* and *APPENDIX B: Mock-ups derived from the interviews*). These paper-based mock-ups were then used in the first Persona, Scenario, and User Journey Workshop to develop concrete User Journeys for three personas. After the workshop, the paper-based mock-ups were reworked, and new mock-ups were developed so that the EMERALD can fulfil the activities developed in the workshop (see *APPENDIX C: User Journeys and paper-based Mock-ups*). From autumn 2024 until March 2025, we conducted further workshops with the pilot partners. We conducted process workshops (see D4.2), to better understand the audit preparation processes. In these workshops, we also presented the clickable mock-ups to collect feedback and input to improve the mock-ups. From June 2025 to September 2025, we conducted further workshops with the pilot partners regarding the reporting functionality. Again, during these workshops, we presented the latest status of the clickable mock-ups and asked for feedback and input.
- **Component owners**: Subsequently, a series of workshops was conducted with the individual component partners of EMERALD. Two workshops were conducted with each component partner. In the first workshop, the EMERALD component was presented, followed by a discussion on how to integrate the component into the EMERALD UI. Based on these discussions, the existing paper-based mock-ups were elaborated in-depth and implemented in Figma[1] (see Section 4). During autumn 2024 and summer 2025, we conducted further workshops with the component owners. The goals were to discuss the clickable mock-ups, the integration of the respective components and to identify potential gaps.

[1] Figma: https://www.figma.com

2.1 Interview with Pilot Partners

With these interviews, we aimed to elicit UX/UI requirements for EMERALD by engaging our target user groups, i.e., (internal) auditors, chief information security officers (CISO), compliance managers. Through the interviews, in-depth insights about the target users' working tasks and activities regarding continuous cloud auditing processes were elicited. Thus, we aimed to gain: i) a solid 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) insights about the users' background knowledge, especially regarding artificial intelligence (AI) (as some parts of EMERALD will use AI technologies).

After having analysed the interview results, the first set of work processes were derived, and an initial set of requirements was developed – more details can be found in D4.2 [14]. Moreover, a first set of paper-based mock-ups were created that served as an initial starting point for the future EMERALD UI/UX.

A detailed description of the interviews, the derived work processes and the corresponding UI/UX requirements can be found in D4.2 [14].

2.2 Personas, Scenarios, and User Journeys Workshops

Based on the insights gained from the interviews and the focus groups, e.g., what the audit preparation processes and audits in general look like, which persons and roles are involved in these processes and what information is needed, a first *Personas, Scenarios, and User Journey* workshop was organised. Table 2 gives an overview of the conducted workshops. The goal of these workshops was to develop detailed personas, scenarios, and user journeys on how the target groups will use the EMERALD UI/UX and which functionalities should be available. Details about the final developed personas and scenarios can be found in D4.2 [14].

Table 2. List of the Personas, Scenarios and User Journeys Workshops

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

After having created personas and scenarios, user journeys can be easily developed [15]. User journeys illustrate how a user interacts with a system step-by-step, incorporating their emotions to identify the needs of the intended application or tool. User journeys help designers and businesses understand the user's needs, motivations, and potential pain points throughout their interaction. This visual representation can highlight gaps in the user experience, leading to targeted improvements in functionality and satisfaction. By employing techniques like journey mapping, organizations can better empathize with users and refine their offerings to enhance

usability and engagement [16], [17]. Consequently, well-crafted user journeys are instrumental in fostering user-centric development and driving successful outcomes.

2.2.1 Procedure

To invite participants to the workshop, we contacted the pilot partners and all members of WP4 and WP5 by email. The Personas, Scenarios, and User Journeys workshop was conducted online using MS Teams. To facilitate collaboration, we used Miro[2], an online collaborative whiteboard.

The first workshop was conducted on two different days, i.e., in two parts (see Table 2). In the first part of the workshop, four different personas were developed. In the second part of the workshop, for three out of the four personas, concrete scenarios were developed. More information about the personas and the scenarios developed in the **Personas, Scenarios, and User Journeys Workshop Part I can be found in D4.2** [14].

Personas, Scenarios, and User Journeys Workshop Part II: The second part of the workshop was attended by 9-11 participants. After the development of the three scenarios for the personas Emerson, Dylan, and Charlie, three corresponding User Journeys were developed. To do so, we asked the participants to divide each scenario into individual steps. For each of these individual steps, the participants were asked to describe the interactivity of the persona with the EMERALD UI. For this task, they should consider the prepared paper-based mock-ups – either as inspiration for the interaction with the EMERALD UI or to add concrete suggestions or ideas of how the EMERALD mock-ups should be further developed or which functionalities to add. To guide the development of the User Journeys, we developed a template (see Figure 2) consisting of three parts:

- Scenario steps: the upper part of the template allows to split the scenario into different steps (see Figure 2, point 1).
- Interaction with the EMERALD UI: For each step of the scenario, a description of the interaction with the EMERALD UI should be added (see Figure 2, point 2).
- Mock-ups: Below we have added some mock-ups that might fit to the corresponding scenario (see Figure 2, point 3).

[2] Miro: https://miro.com/

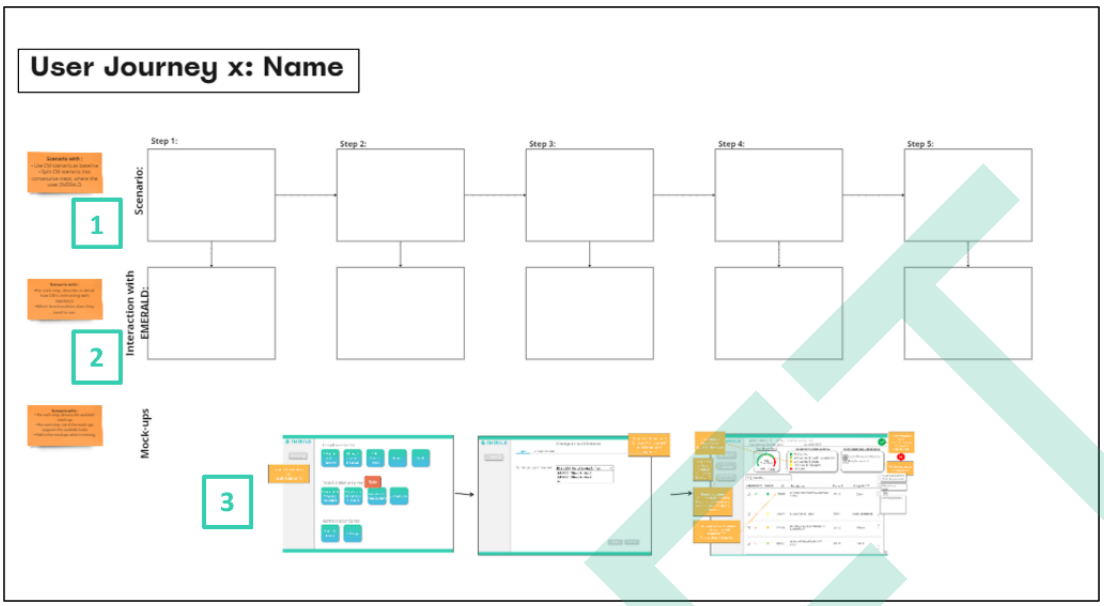

Figure 2. Template for developing the User Journeys

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

Before the workshop, we updated the EMERALD Miro board to support the development of personas. In a brief meeting with NIXU/DNV colleagues, we explained our goals, the use of the board, and introduced two templates from previous workshops. They then created personas and scenarios independently. In the following workshop, we reviewed and refined their work, resulting in two new personas: Jarkko, a lead auditor, and Eero, a technical auditor, both from a consulting company presented in D4.2 [14]. In this workshop, no user journeys were developed.

Final Personas, Scenarios & User Journey Workshop Part III: Twelve participants attended the final workshop. Before inviting all EMERALD partners, we reviewed D5.1 [18] to identify stakeholders involved in the pilot setup. We compiled a table of these stakeholders and, with the consortium, determined which were relevant to EMERALD and which were missing. This informed the final workshop, where we used a structured Miro board to address remaining gaps—one persona, several scenarios, and especially all user journeys—using templates documented in D4.2 [14] (Figure 2) and D4.3 [1] (Figure 2).

Table 3 reflects the final status upon completion of all workshops, including all developed user journeys.

Table 3. Status Overview of the Development of Personas, Scenarios and User Journeys.

	Roles	Notes	Personas	Scenarios	User Journeys
Compliance Stakeholders	Compliance Manager	UI/UX: they will be merged in one role in the EMERALD UI	Riley	5	4
	Compliance Manager for financial services		Emerson	1	1
	Internal Control Owner	-	Dylan	1	1

	Roles	Notes	Personas	Scenarios	User Journeys
Technical Stakeholder	Technical Implementer	One role covering all technical roles including the metric implementer, developers, etc. (Old name: Metric Implementor)	Morgan	2	1
Auditor Stakeholders	Internal Auditor	-	Charlie	1	1
	External Lead Auditor	UI/UX: they will be merged in one role in the EMERALD UI	Jarkko	4	4
	External Technical Auditor		Eero	2	2

The workshops resulted in altogether 14 different user journeys. We will present all of them in detail in Section 3.

2.3 EMERALD UI & Component Owner Workshops

Following interviews and focus groups with pilot partners, along with workshops focused on personas, scenarios, and in particular, user journeys, we launched a dedicated workshop series involving all EMERALD component owners (see Table 4). The goal of this workshop series is to find out how to integrate all EMERALD components into the EMERALD UI.

Table 4. Overview of the Workshops: EMERALD UI & Components

Component (Owner)	Part I	Part II	Part III	Part IV
Workshops with Major Component Owners				
AMOE (FABA)	31.07.2024	22.08.2024		
Orchestrator (FhG)	31.07.2024	11.10.2024		
MARI (CNR)	23.07.2024	09.10.2024	17.10.2024	10.02.2025
RCM (TECNALIA)	24.07.2024	10.09.2024		
TWS (TECNALIA)	01.08.2024	26.08.2024		
Workshops with Evidence Extractor Component Owners				
eknows-e3/Codyze (SCCH / FhG)	09.10.2024	10.12.2024		
AI-SEC (FhG)	30.10.2024			
Clouditor Discovery (FhG)	07.11.2025			
Additional Workshops				
All Component Owners	12.02.2025			
Self-Assessment Questionnaire - EUCS (TECNALIA)	13.03.2025	09.5.2025	26.05.2025	
Audit Scope UI (WP4) & Exploitation Workshop (WP6) (FABA)	07.04.2025			
Audit Scope (FhG & FABA)	09.04.2025	04.06.2025		
Further Functionalities and Features (FhG & FABA & TECNALIA)	18.09.2025			
Final Mock-ups Workshop (ALL)	23.09.2025			

2.3.1 Workshops with Major Component Owners: Procedure

To set up the workshop series, we sent out an invite to the EMERALD component owners of AMOE (FABA), Orchestrator (FhG), MARI (CNR), RCM (TECNALIA), and TWS (TECNALIA). We asked them to fill in a Doodle to schedule two dates for each component. The first workshop date for each component meeting (Workshop – Part I) was set for the last two weeks of July and the beginning of August 2024. The second workshop series (Workshop – Part II) took place at the end of August and mid of September 2024. In all workshops, we used Miro[3] as an online collaborative whiteboard. With TECNALIA & RCM we conducted an additional workshop in October 2024 (Workshop Part III) and another one in February 2025 (Workshop – Part V).

Workshop (Part I): Each workshop followed the same structure. At the beginning of each workshop, we presented the goal of the workshop namely to find out how to integrate the EMERALD component into the EMERALD UI. For each of the components, we created a Miro board with three different frames as presented in Figure 3. In the first Miro frame, we shortly summarized the purpose of the respective component. During the initial discussion round, we engaged with each component owner to confirm our understanding of their component's purpose and to uncover any uncertainties. Following this, we engaged with each component owner to explore UI integration from two perspectives: first, the setup process of the component, if necessary, and second, its integration into the UI during user interaction.

- "Set-up" of the component: In the second frame of the Miro Board, we made available predefined mock-ups of the EMERALD landing page, possibilities to set up EMERALD, as well as neutral mock-ups. Then we discussed with the component owner step-by-step what was needed for setting up the component (if necessary), asking questions such as: Which information is needed to set up the component? Which information should be presented in the UI? Which functionality should be offered by the UI?
- "Working" with the component: In the third frame, we added on the one hand mock-ups we have prepared regarding how we thought the component could be integrated into the UI. On the other hand, we again added empty mock-ups to leave room for innovation and creativity. Again, we asked similar questions regarding the visualisation and functionality.

Workshop (Part II): The goal of each follow-up workshop was to present the created clickable prototypes developed in Figma[4] to discuss if they work in a way that is in line with what the component owners would like to have and if the prototype fulfils all required functionalities. Similar to the first workshop, we first presented the results from two perspectives – the set-up phase (where applicable) and the working phase. As those phases were strongly dependent on the different components, the workshops were tailored to the component owners' needs and the component's integration into the UI. For example, to set up a cloud service, registered evidence extractors need to be added to the cloud service to retrieve the assessment results from Clouditor-Orchestrator. For AMOE no set-up is necessary, and it must be possible to upload the respective policy documents for the different controls or schemes.

Workshop (Part III): Based on the workshops done before, we met again to discuss with the project partners the implementation of the MARI and RCM Tool in Figma. We clicked step-by-step through the respective mock-ups, to see if we understood the partners' needs correctly. We received a lot of feedback and further suggestions on how to improve the integration and how to combine the smooth interplay between both tools.

[3] Miro: https://miro.com/
[4] Figma: https://www.figma.com

Workshop (Part IV): After several months, when the clickable mock-ups had been significantly improved, we reconvened the workshop. Again, we went through the clickable mock-ups to discuss if their implementation fulfils the needs of the component owners of RMC and MARI.

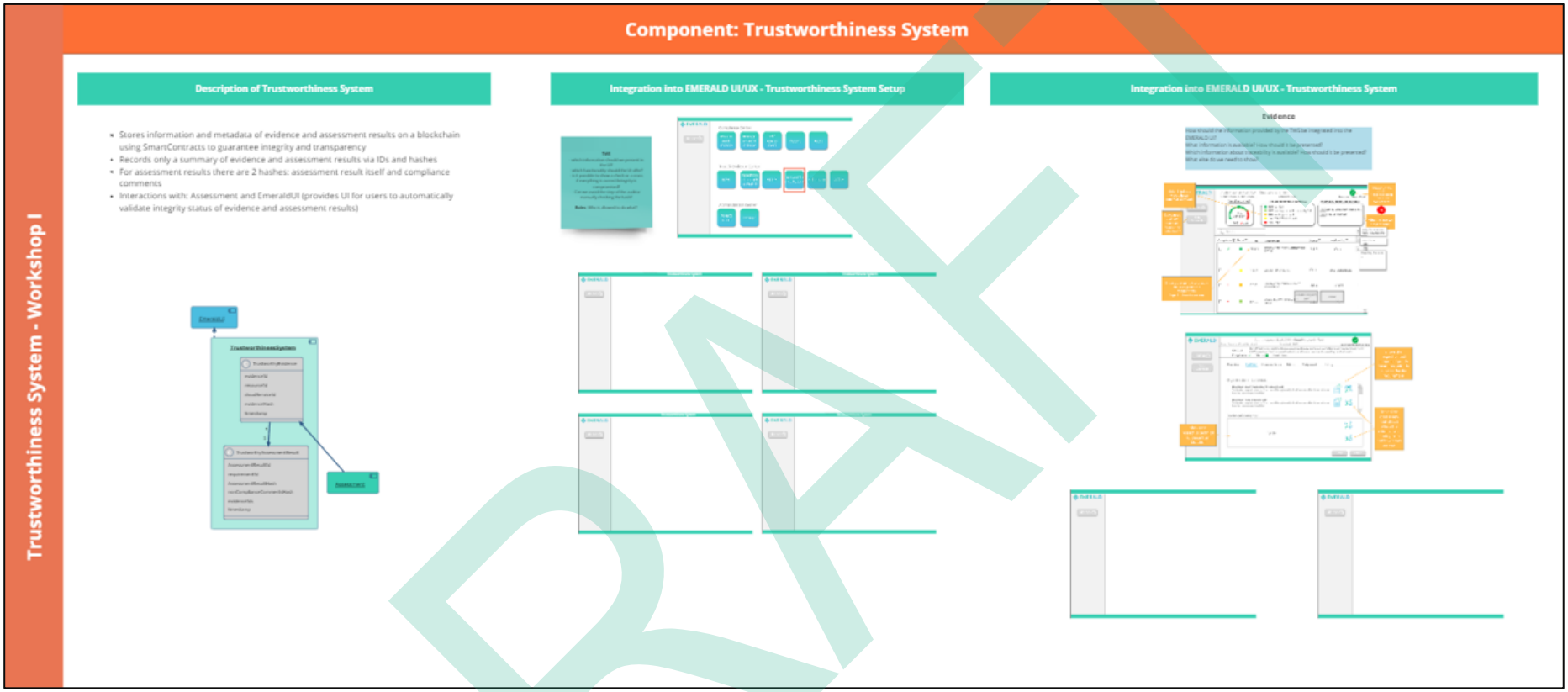

Figure 3. Example of a prepared Miro board for TWS with the three different frames

2.3.2 Workshops with Evidence Extractor Component Owners: Procedure

In autumn 2024, we got in contact with the owners of the different evidence extractors to find out to what extent the evidence extractors could or should be integrated into the EMERALD UI. For eknows-e3 (SCCH) and Codyze (FhG) two meetings were conducted, while for Clouditor Discovery (FhG) and AI-SEC (FhG) only one meeting was necessary. In all meetings, we presented the current status of the clickable mock-ups to the participants and how we envisioned integrating the evidence extractors. Thereupon, we started a discussion with the participants, collected their input and feedback. Afterwards, we implemented the requested changes and presented the results either in a second workshop meeting or in a bi-weekly WP4 meeting.

2.3.3 Additional Workshops with Component Owners: Procedures

Workshop with all component owners: In February 2025, we invited all component owners to participate in an online workshop. In this workshop, we presented the current status of the clickable mock-ups to the component owners and guided them step-by-step through the different parts of the EMERALD UI. For each part, we asked them for feedback about how we integrated the respective components in the UI, if something was missing, if something else was needed or if they had other ideas. All feedback received was noted down and later implemented in the clickable mock-ups (if feasible).

Audit Scope Workshops with FhG and FABA: At the General Assembly Meeting in Pisa (March 2025), a discussion was initiated on how to improve the audit scope view as it did not represent all relevant stati necessary for continuous compliance-as-a-service for cloud services. Subsequently, several meetings took place. The first meeting was conducted in April 2025 in Graz with FABA, to get a better understanding of what the audit scope views need to provide to offer a) the possibility to manage the implementation of the controls and b) to offer continuous compliance-as-a-service. Based on these discussions, we prepared a Miro Board – as depicted in Figure 4 – for the next Audit Scope Workshop together with FhG and FABA (April 2025). In this workshop, we discussed the current implementation of the audit scope views and made decisions on how to improve and change them. After having implemented all the discussed points in the clickable mock-ups, we conducted a follow-up meeting in June 2025 with FhG and FABA, where we presented all changes conducted to check if the audit scope views were tailored to accommodate the whole spectrum of a compliance-as-a-service platform. Overall, we came to a final audit scope view that serves all expectations and needs of the component owners and the pilot partners.

Further Functionalities and Features with FhG & FABA & TECNALIA: In this workshop we discussed some specific functionalities and features to clarify if the last changes made in the mock-ups were correct and if something was still missing. We discussed topics such as: MARI/RCM Setting page, History functionality for the certification scheme and audit scope, as well as the audit scope reports. Relevant feedback received was integrated into the mock-ups.

Final Mock-ups Workshop: For the final mock-ups we invited the whole EMERALD consortium. Altogether 10 people participated in the workshop coming from FABA, TECNALIA, CNR, and SCCH. In this workshop we went through the whole clickable mock-ups, showed all features and functionalities to collect final feedback form all consortium partners. Afterwards, the feedback we received was integrated into the mock-ups.

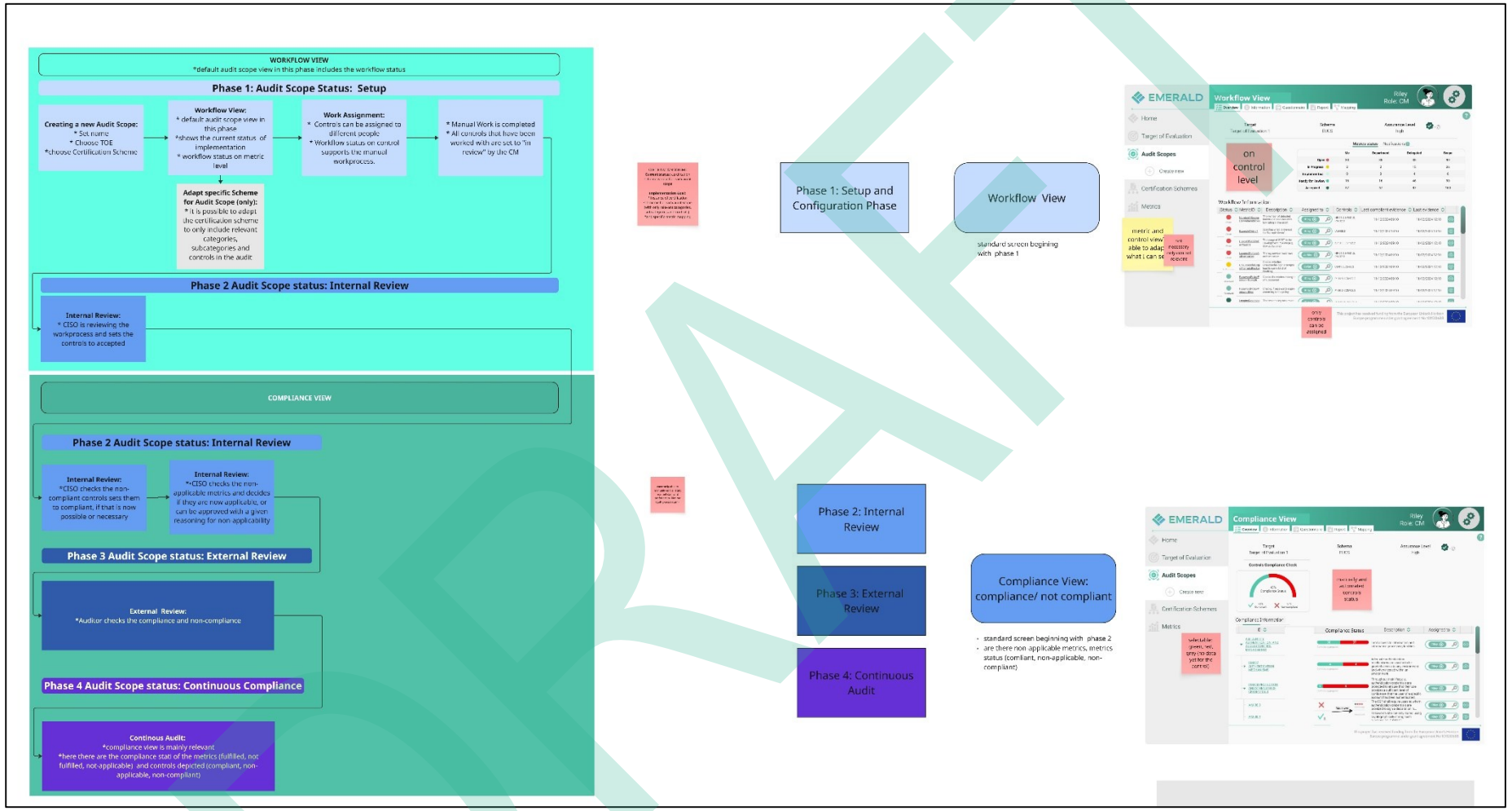

Figure 4. Prepared Miro Board for discussing the Improvements of the Audit Scope Views

Self-Assessment Questionnaire Workshops with TECNALIA: One requirement for the EMERALD UI was the provision of a self-assessment questionnaire for EUCS, which is implemented by TECNALIA. Altogether, we setup 3 different workshops for discussing this questionnaire. In the first workshop, TECNALIA presented the self-assessment questionnaire implemented in the MEDINA project [19], which served as starting point for the clickable mock-up views. Based on these insights, a first version of the questionnaire was implemented and discussed in a meeting mid of May 2025. In this workshop, further requirements about functionalities that the questionnaire should provide were discussed. After having implemented all changes in the clickable mock-ups, another workshop meeting was setup with TECNALIA, to see if the self-assessment questionnaire fulfilled all functionalities and features. After this meeting, we also got some additional requirements for the questionnaire via email and implemented them as well.

2.4 EMERALD UI & Pilot Partner Workshops

In parallel to the different types of workshops with the component owners, we also conducted different workshops with the pilot partners.

Table 5. Overview of the Workshops: EMERALD UI & Processes & Reports

Pilot Partners	Part I	Part II
Workshops about the UI and Processes		
Workshop for UI and processes (CF)	14.11.2024	25.02.2025
Workshop for UI and processes (FABA)	24.02.2025	04.03.2025
Workshop for UI and processes (DNV/NIXU)	28.02.2025	07.03.2025
Workshop for UI and processes (CXB)	04.03.2025	
Workshop for UI and processes (IONOS)	05.03.2025	
Presentation of pilot partner processes (TECNALIA)	03.04.2025	
Workshops about reports		
Mock-ups Review and Report Workshop (FABA Mind breeze)	14.07.2025	
Mock-ups Review and Reports Workshop (FABA)	16.07.2025	
Mock-ups Review and Reports Workshop (CF)	16.07.2025	
Mock-ups Review and Reports Workshop (IONOS)	24.07.2025	

2.4.1 Workshop for UI and processes - Procedure

From the interviews conducted (see Section 2.1), we were able to derive simple processes of the audit (preparation) processes, without and with EMERALD support. To elaborate on these processes, we conducted a series of workshops with all pilot partners IONOS, CF, FABA, CXB and DNV/NIXU. We refined the initial simple processes and created two workflow representations—without and with EMERALD support—for each pilot partner and for the auditors. These were visualized on individual Miro boards. From these, we derived an initial blueprint process intended to unify all partner workflows.

In February/March 2025, we conducted EMERALD UI and process workshops (see Table 3) with each partner and the auditors to review and refine the EMERALD UI and the respective workflows. Based on the collected feedback, we adapted the processes and asked participants for final confirmation. The final versions of the simple processes, workflow processes and the EMERALD blueprint were presented in D4.2 [14]. The feedback we got from the pilot partners and NIXU/DNV regarding the EMERALD UI was implemented in the clickable mock-ups (see Section 4).

2.4.2 Mock-ups review and report workshops - Procedure

In July 2025, we invited the pilot partners and DNV/NIXU again to another series of workshops, aiming at presenting the current version of the EMERALD UI to them. Additionally, we discussed with them which information regarding the audit scopes and the compliance status of controls should be available in downloadable reports (e.g. reports for internal or external audits). To support the discussions about the reports with the pilot partners and DNV/NIXU we again prepared a Miro board (see Figure 5) showing some of our ideas of how such a report could look like. Together with the participants, we discussed the suggestions and adapted them accordingly with the participants' needs and suggestions. More details about the developed reports are presented in Section 4.5.3.4.

Figure 5. Prepared Miro board for discussing the downloadable Reports

2.5 EMERALD Terminology

During the development of the paper-based and clickable mock-ups, the consortium discussed and unified the naming convention for the whole EMERALD project. “Certification target” is a (cloud) service that will be certified according to a specific certification scheme; it represents what a system or service does and how it does it (including the architecture). In the last GA in spring 2025 the naming convention was again discussed, and the consortium decided to call the “Certification target” now “Target of Evaluation (ToE)”.

The “target of evaluation” (ToE) comprises all relevant entities for a solid security posture and resilience to risk. This includes (cloud) infrastructure resources, source code or binary code of deployed services, documents detailing company processes as well as other services offered to customers, like AI models.

“Audit scope” (previously called audit instance) refers to the scope of an individual audit. It includes the Target of Evaluation (i.e., a sub-selection of resources, documents detailing processes and Source code/Binaries of cloud SW) set into context of relevant controls from relevant Security schemes. More information about the EMERALD terminology can be found in the EMERALD glossary in D1.4 [20].

As the development of the EMERALD terminology took place after the development of the first paper-based mock-ups, the paper-based mock-ups presented in the appendixes (*APPENDIX A: Mock-ups derived from Interviews with Pilot Partners*, *APPENDIX B: Mock-ups derived from the interviews, and APPENDIX C: User Journeys and paper-based Mock-ups*) contain the previous terminology – namely “audit instance” (instead of audit scope) and certification target.

The clickable mock-ups (see Section 4) are using the consolidated EMERALD terminology.

3 EMERALD User Journeys

The Personas, Scenarios, and User Journey workshops were conducted between June 2024 to October 2024. These workshops resulted in altogether seven different personas divided into three stakeholder groups and 16 concrete scenarios. A detailed description of the personas and scenarios can be found in D4.2 [14].

3.1 Summary of Personas and Scenarios

In this section, a short summary of the developed personas and scenarios are presented. The detailed results of the developed personas and scenarios are reported in D4.2 [14].

Altogether seven different personas were developed, which are summarised below along the different stakeholder groups:

Compliance Stakeholders:

- **Riley – Cloud Service Compliance Manager**: Riley is a junior compliance analyst whose responsibilities are organizing audits and managing the scheduling of different compliance schemes. 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. Riley's pain points refer to i) reliance on others to finish tasks timely, ii) lack of efficient audit tools, and iii) lack of understanding of complex certification frameworks. EMERALD should help Riley with the day-to-day tasks by speeding up the work.

- **Emerson – Compliance Manager in Financial Services Institution**: Emerson focuses on risk management of third-party cloud services, assesses controls based on risk and regulation, manages contractual agreements, and monitors compliance. The overall goal of Emerson is to ensure i) that all service providers are compliant with given standards, and ii) safety by mitigating risks associated with audit requirements. Challenges refer to the communication across departments. EMERALD could help in the day-to-day tasks by providing a centralized point for evidence, metrics, and controls, by automating tedious processes and management of numerous audits and reducing the workload.

- **Dylan – Internal Control Owner**: Dylan is an experienced product owner and is responsible for leading the head of production team and overseeing and planning product development and backend services. Regarding audits, Dylan's tasks consist of defining metrics, collecting evidence for implementing controls, assigning and delegating control implementation to the team aiming at having all controls for services compliant. EMERALD could help Dylan by allowing to i) simply delegate tasks, ii) provide an overview of assigned controls and iii) display assessment results.

Technical Stakeholder:

- **Morgan – Technical Implementer:** Morgan is a DevOps expert and is responsible for the technical implementation of metrics, deploying new cloud services, and adjusting

configurations to align with security policies. Additionally, Morgan has to setup verification mechanisms as well as install roll-back mechanisms and is responsible for system configuration tasks. EMERALD should provide Morgan a ToDo List, allow to check the status of controls and evidence, and provide the possibility to assign controls and metrics to other colleagues. It should offer a history view of changes regarding metrics and should allow to check the status of the certificate.

Auditor Stakeholders:

- **Charlie – Internal Auditor**: Charlie is a senior auditor, and Charlie's responsibilities include managing the audit process, planning, reporting, and maintaining contact with customers. Charlie offers templates to the customers/colleagues with the goal to i) provide easy access to information/evidence, ii) reduce risks, iii) fulfil audit KPIs, and iv) help customers. Challenges refer to getting in contact with the responsible person and retrieving the relevant information. The EMERALD UI could help by providing an overview of the required information and support the creation of respective reports.

- **Eero - Technical Auditor**: Eero is a technical auditor of an external audit company. Eero's tasks involve the identification of attack paths, the improvement of customer systems and their components, enhancing cybersecurity through hardening measures, and conducting technical analyses using both tools and manual methods. For Eero, EMERALD should provide a clear distinction between manual and automated tests, including a task list for manual testing. It should allow manual enrichment of automated test results, such as marking false positives or adding detailed outcomes.

- **Jarkko – Lead Auditor**: Jarkko's tasks include ensuring an adequate scope, selecting the correct assurance level from the certification scheme, identifying appropriate controls, and verifying that the chosen metrics align with the assurance level of the selected certification scheme. Additionally, it involves auditing implemented controls, reporting findings, and making certification decisions. The EMERALD UI should allow auditors to adjust metrics target values and organizational metrics if they are deemed inadequate. Manual evidence can be added via the UI to supplement automated evidence, and auditors should be able to extract responsibility information from policy documents and track their update frequency.

Altogether 16 scenarios have been developed for the seven different personas. Here we only provide a tabular overview of each scenario. The detailed scenarios can be found in D4.2 [14].

Table 6. Overview of Personas and their Scenarios

Stakeholder groups	Persona	Scenario
Compliance Stakeholders	Riley	• Scenario A: Riley – Managing a New Audit Scope • Scenario B: Riley – Manage all Controls of an Audit Scope • Scenario C: Riley – Uncover all "blind spots" • Scenario D: Riley – Updating a certification scheme • Scenario E: Riley – Accompanying an Audit
	Emerson	• Scenario: Emerson – Bring Your Own Certification Scheme
	Dylan	• Scenario: Dylan – Internal Control Owner Control Implementation
Technical Stakeholder	Morgan	• Scenario A: Morgan – Checking Metrics and Evidence • Scenario B: Morgan – Removal of Metrics
Auditor Stakeholders	Charlie	• Scenario: Charlie – Preparation of an Audit by an Internal Auditor
	Jarkko	• Scenario A: Jarkko – Scoping • Scenario B: Jarkko – Preparing for Audit • Scenario C: Jarkko – Organizational Audit • Scenario D: Jarkko – Certification
	Eero	• Scenario A: Eero – Technical Audit • Scenario B: Eero – Reporting

Please note that Riley's *"Updating a certification scheme"* and Morgan's *"Removal of Metrics"* scenarios do not require dedicated user journeys because they will not be implemented in the EMERALD UI.

3.2 User Journeys

This section provides a detailed description of the user journeys we have developed for EMERALD. The journeys are presented in a logical order that reflects their relevance to the overall workflow and system implementation.

Three of the User Journeys were already introduced in deliverable D4.3 [1] but have been adapted to align with updated naming conventions and changes in the technical implementation. Over time, the User Journeys have evolved in parallel with the EMERALD UI development to ensure consistency between design and functionality.

As we have continuously worked on the EMERALD UI, we have implemented the user journeys directly in the clickable mock-up. Thus, we have not developed new paper-based mock-ups. In D4.3 [1], we presented three additional user journeys and the created paper-based mock-ups, which have been included in this deliverable in *APPENDIX C: User Journeys and paper-based Mock-ups*.

All relevant User Journeys are presented in detail below. For each user journey, we first describe the tasks a persona must perform followed by the interaction with the EMERALD UI.

3.2.1 Riley – Managing a New Audit Scope

The scenario "Managing a New Audit Scope" for Riley was divided into the following six steps, as depicted in Figure 6.

Step 1 – Uploading a New Certification Scheme:

- **Riley's Tasks:** Riley opens the EMERALD framework and uploads the necessary file for the new certification scheme (using RCM).
- **Interaction with the EMERALD UI**: Riley opens the EMERALD UI in their web browser and signs in with their credentials. They go from the landing page to the certification scheme overview and select "create scheme" to upload a new scheme (file).

Step 2 – Browsing the New Certification Scheme:

- **Riley's Tasks:** Riley browses the newly created BSI C5 certification scheme. Riley investigates the categories and controls in detail.
- **Interaction with the EMERALD UI**: Riley clicks on the BSI C5 scheme to gather more information about the scheme. Riley clicks on a category to investigate the controls. For each control, the related metrics and implementation guidelines are also available.

Step 3 – Mapping the New Certification Scheme:

- **Riley's Tasks:** Riley navigates to the Control Mapping to check which controls of the previously used EUCS scheme correspond to controls in the new scheme "BSI C5". Riley makes a mapping between controls and takes over the corresponding metrics from EUCS. The mapping is stored in RCM.
- **Interaction with the EMERALD UI**: In the certification scheme overview, Riley navigates to the control mapping and selects the already mapped scheme (EUCS) on the right-hand side to map those to similar controls to the newly uploaded certification scheme on the left-hand side (BSI C5). Additionally, Riley accepts to also take over the metrics.

Step 4 – Creating a New Target of Evaluation:

- **Riley's Tasks:** Riley sets up the target of evaluation (e.g., the cloud solution (including TWS configuration, access rights, resources, processes, and source code/ binaries) that will be audited), sets up all relevant EMERALD extractors, and, if possible, uploads all relevant policy documents regarding the current target of evaluation.
- **Interaction with the EMERALD UI**: Riley returns to the landing page, clicks on "Target of evaluation", and then clicks on "Create new". They enter all the relevant information, e.g., title and description. Then, they download the instructions for the relevant evidence extractors and upload all relevant policy documents.

Step 5 – Creating a New Audit Scope:

- **Riley's Tasks:** Riley creates an audit scope using the respective target of evaluation and the new certification scheme and checks the respective assessment results and evidence retrieved so far.
- **Interaction with the EMERALD UI**: Riley returns to the landing page and clicks on "Audit scopes". They click on "Add new". They enter the audit scope name, select the target of evaluation they created in the prior step, and select the certification scheme that will be used for this audit.

Step 6 – Managing the Audit Scope:

- **Riley's Tasks:** Riley is using the newly created audit scope to manage the newly required certification schema for the selected cloud service (ToE).
- **Interaction with the EMERALD UI**: Riley sees the overview of the newly created audit scope and can now proceed with further actions on this scope.

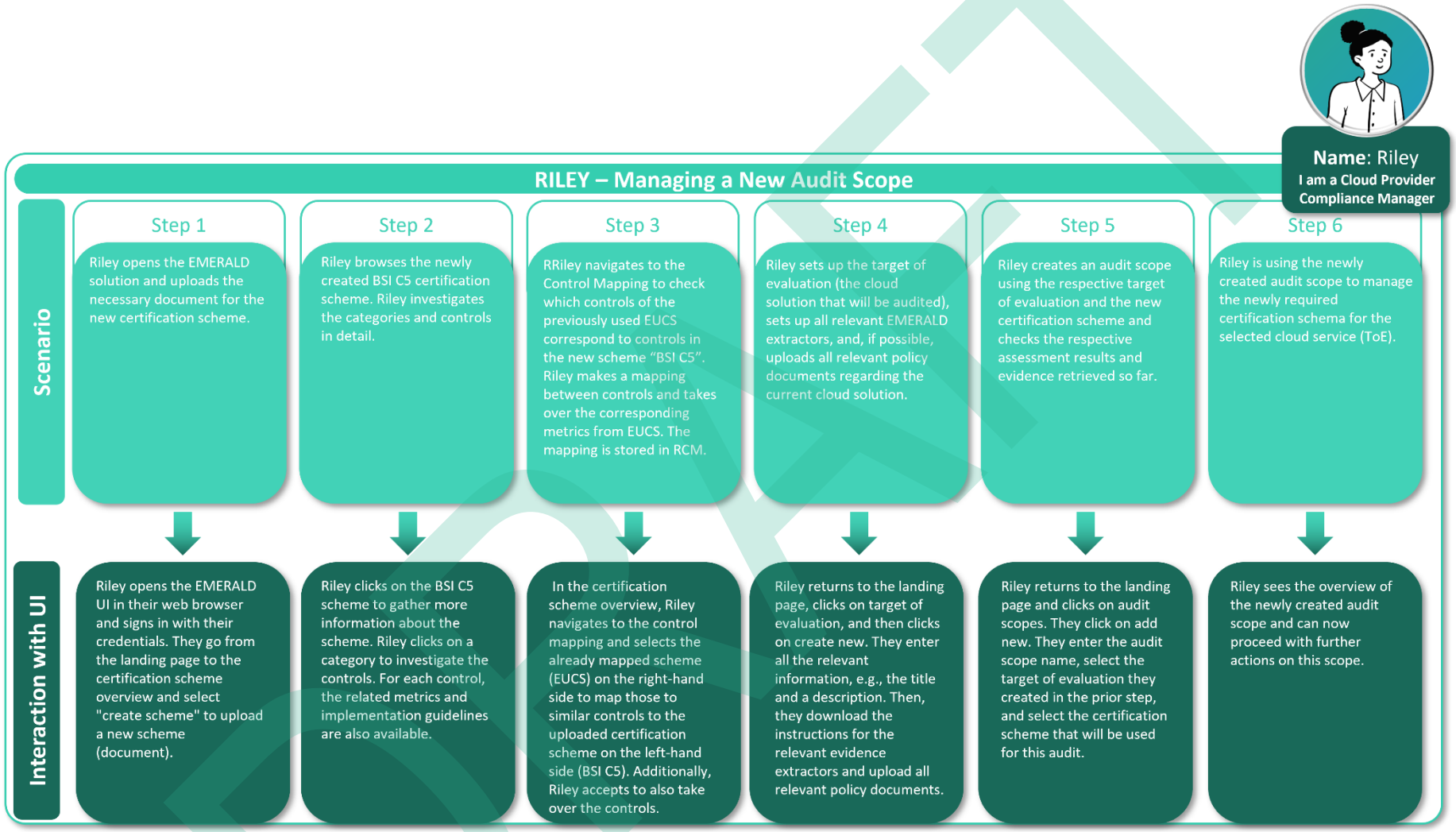

Figure 6. Riley – Managing a New Audit Scope

3.2.2 Riley – Manage all Controls of an Audit Scope

The scenario "Managing all Controls of an Audit Scope" for Riley was divided into the following five steps, as depicted in Figure 7.

Step 1 – Open the Audit Scope:

- **Riley's Tasks:** Riley opens the corresponding audit scope in the EMERALD framework and checks the compliance status for all controls.
- **Interaction with the EMERALD UI**: Riley opens the EMERALD UI in their web browser and signs in with their credentials. They click on the audit scope and select the audit scope they want to focus on.

Step 2 – Filter Controls:

- **Riley's Tasks:** Riley wants to get a good overview of the audit scope. Therefore, they filter the controls based on their different workflow states and compliance states.
- **Interaction with the EMERALD UI**: Riley uses the filter functionality in the process view and in the compliance view to filter the controls according to their current states.

Step 3 - Review Workflow Status:

- **Riley's Tasks:** Riley checks the workflow state of the controls and can neglect all controls that are already accepted (marked with a dark green check). All other controls still need to be worked on by the team.
- **Interaction with the EMERALD UI**: In the process view, Riley uses the workflow filter functionality to display items with the states "Open," "In Progress," "Implemented," and "Ready for Review," allowing them to easily track everything that still requires implementation or review.

Step 4 - Identify Non-Compliant Controls:

- **Riley's Tasks:** Riley checks the compliance state of the controls and can neglect all controls that are compliant (marked with a green check mark). Non-compliant controls require follow-up from the team. Riley needs to decide what to do: Step 5a OR Step 5b.
- **Interaction with the EMERALD UI**: With the filter functionality for the compliance status in the compliance view, Riley filters for the state "not compliant" and can see all the controls that are not compliant.

Step 5a - Assign a Control for Implementation:

- **Riley's Tasks:** Riley checks the compliance state of the controls and can neglect all controls that are compliant (marked with a green sign). Controls that are not compliant require follow-up from the team.
- **Interaction with the EMERALD UI**: Riley clicks on a specific control and assign this control to the respective person. Riley can additionally add a comment to provide some further insights.

Step 5b - Gather More Information Before Assignment:

- **Riley's Tasks:** Riley opens the respective control to get more information about the assessment result available; this may give Riley further insights, who is the right person to manage the control further.
- **Interaction with the EMERALD UI**: Riley clicks on the specific control and sees a list of metrics and their assessment results. They can also get further details regarding the

evidence when clicking on the metric. Then Riley edits the control to assign this control to the respective person. Riley can additionally add a comment to provide some further insights.

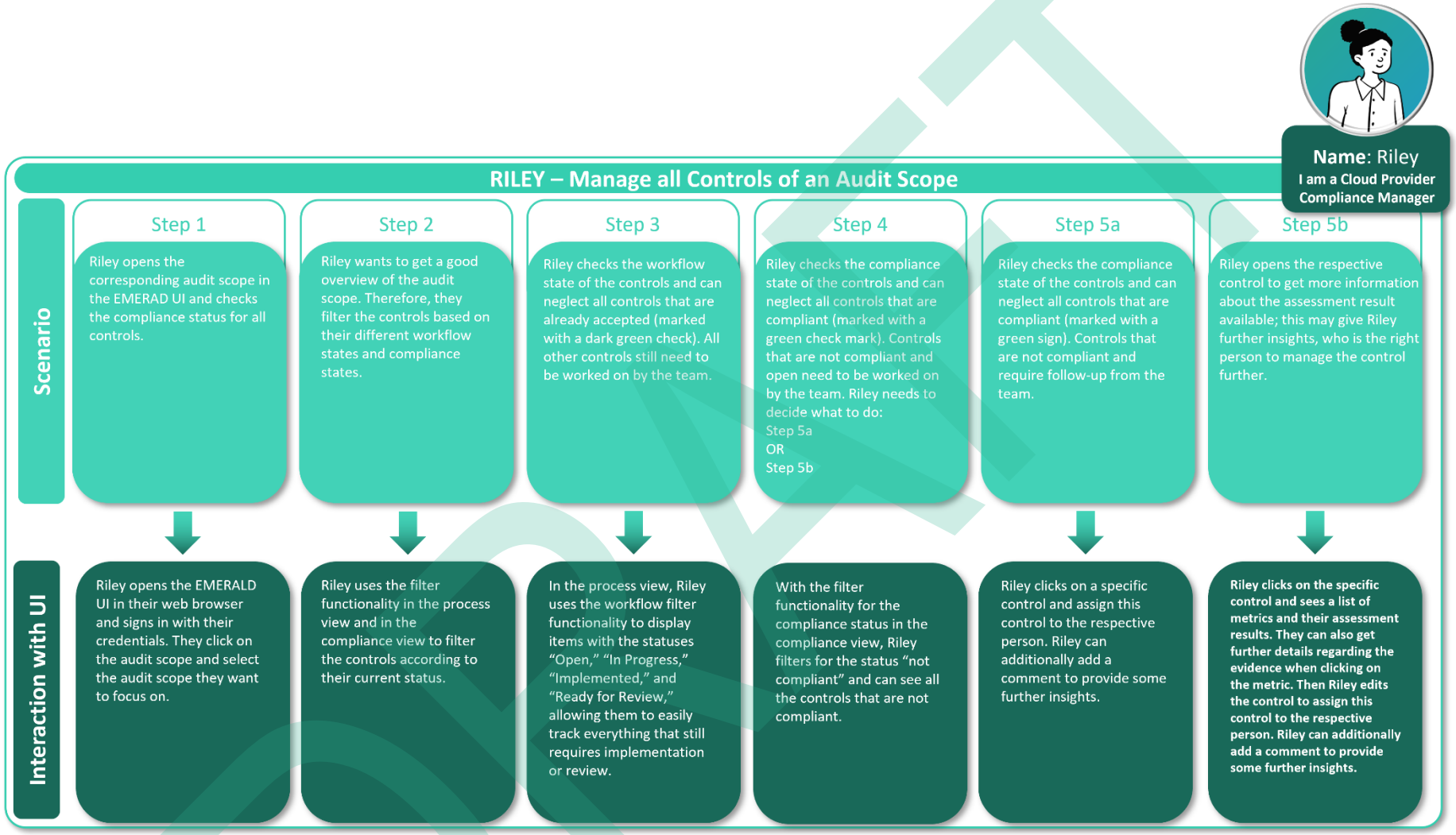

Figure 7. Riley – Manage all Controls and Audit Scope

3.2.3 Riley – Uncover all "blind spots"

The scenario "Uncover all 'blind spots'" for Riley was divided into the following four steps, as depicted in Figure 8.

Step 1 – Audit Scope Preparation:

- **Riley's Tasks:** When preparing for an audit, Riley is responsible that all controls are compliant, and no 'blind spots' (open controls) are left.
- **Interaction with the EMERALD UI**: no interaction required.

Step 2 – Filter Controls:

- **Riley's Tasks:** If Riley finds during their work some open controls, these controls need to be directly addressed. Riley needs to make sure that Step 3a, Step 3b, and Step 3c are fulfilled.
- **Interaction with the EMERALD UI**: Riley opens the EMERALD UI in their web browser and signs in with their credentials. They click on audit scope and select the audit scope they want to focus on, and filters for open controls.

Step 3a – Assignment check:

- **Riley's Tasks:** Riley checks that all controls are assigned to someone.
- **Interaction with the EMERALD UI**: Riley filters in the control list for controls that do not have anyone assigned to them via the "Assigned to" field.

Step 3b – Compliance Status Check:

- **Riley's Tasks:** Riley checks that all controls are either set to compliant or non-compliant.
- **Interaction with the EMERALD UI**: For this Riley checks all controls in the compliance status pending and checks if they can be set manually to compliant or non-compliant.

Step 3c – Verification of Work:

- **Riley's Tasks:** Riley verifies that a colleague has been assigned to manage the pending and non-compliant controls.
- **Interaction with the EMERALD UI**: Riley filters the list of controls in the overall view to display controls that are both non-compliant and unassigned.

Step 4 – Escalation Plan:

- **Riley's Tasks:** After these steps, Riley handles communication, follows up as needed, and initiates an escalation plan when required.
- **Interaction with the EMERALD UI**: Riley can add comments when assigning someone in each of the steps 3a, 3b, and 3c to better structure their following communication.

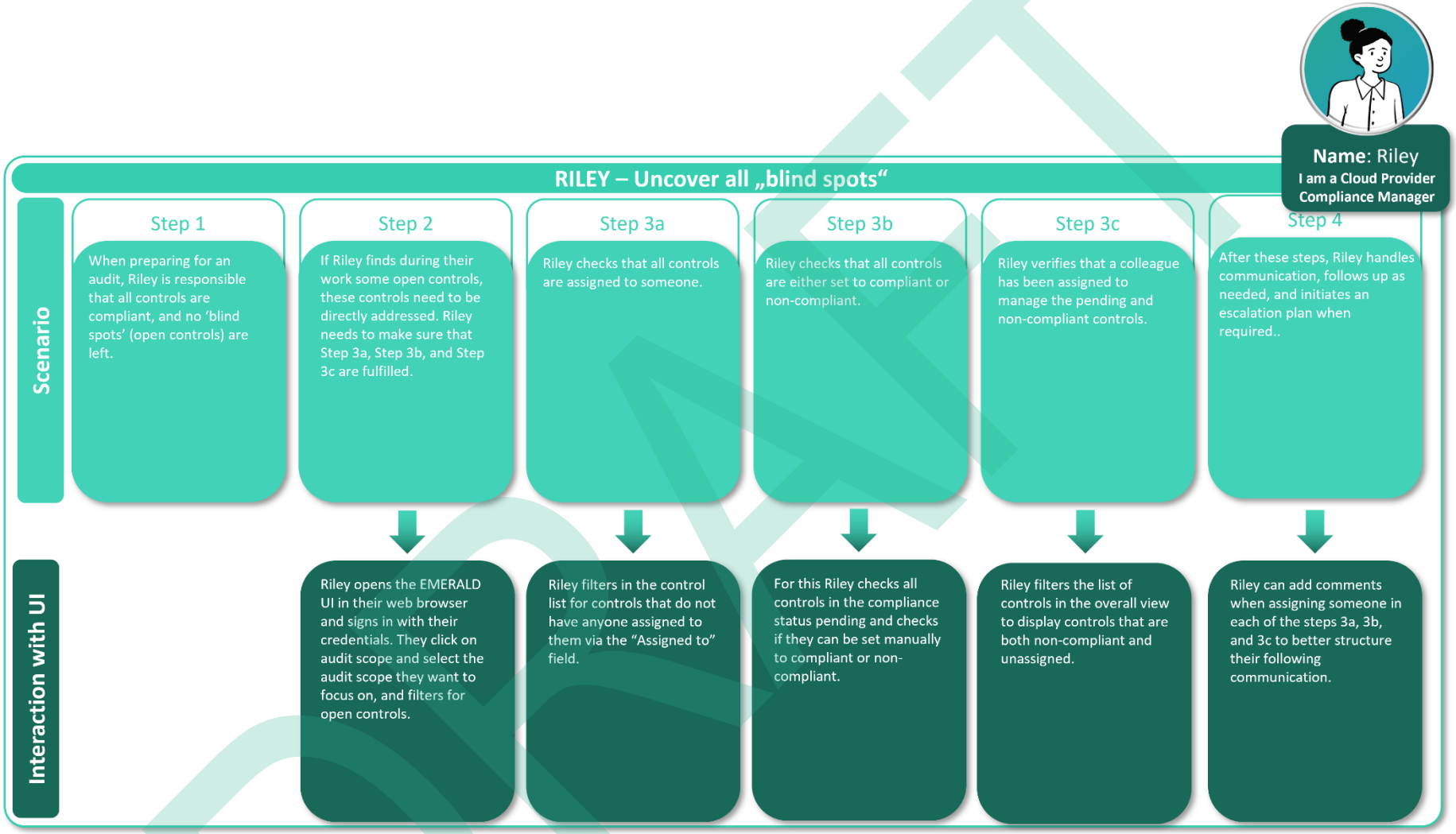

Figure 8. Riley – Uncover all "blind spots"

3.2.4 Riley – Accompanying an Audit

The scenario "Accompanying an Audit" for Riley was divided into the following three steps, as depicted in Figure 9.

Step 1 – Audit Evidence Preparation:

- **Riley's Tasks:** The lead auditor has already selected a big sample of controls for being checked during the audit. Riley has to show the auditor that their cloud system is compliant with the selected controls.
- **Interaction with the EMERALD UI**: no interaction required.

Step 2 – Metric Assessment:

- **Riley's Tasks:** Riley enters the EMERALD UI, looks for the selected controls and shows the auditor the individual metrics and corresponding assessment results for the controls.
- **Interaction with the EMERALD UI**: Riley opens the EMERALD UI in their web browser and signs in with their credentials. They click on audit scope and select the audit scope they want to focus on. Riley selects a control and shows the assessment result of the metrics for the selected control.

Step 3 – Show Evidence:

- **Riley's Tasks:** Riley opens the different assessment results and evidence in EMERALD. Riley shows the auditors, for example, in the policy documents, how the different controls and the respective metrics have been addressed.
- **Interaction with the EMERALD UI**: Riley can select different controls and the respective metrics. Riley also shows the documents associated with this metric and the extracted assessment results and evidence.

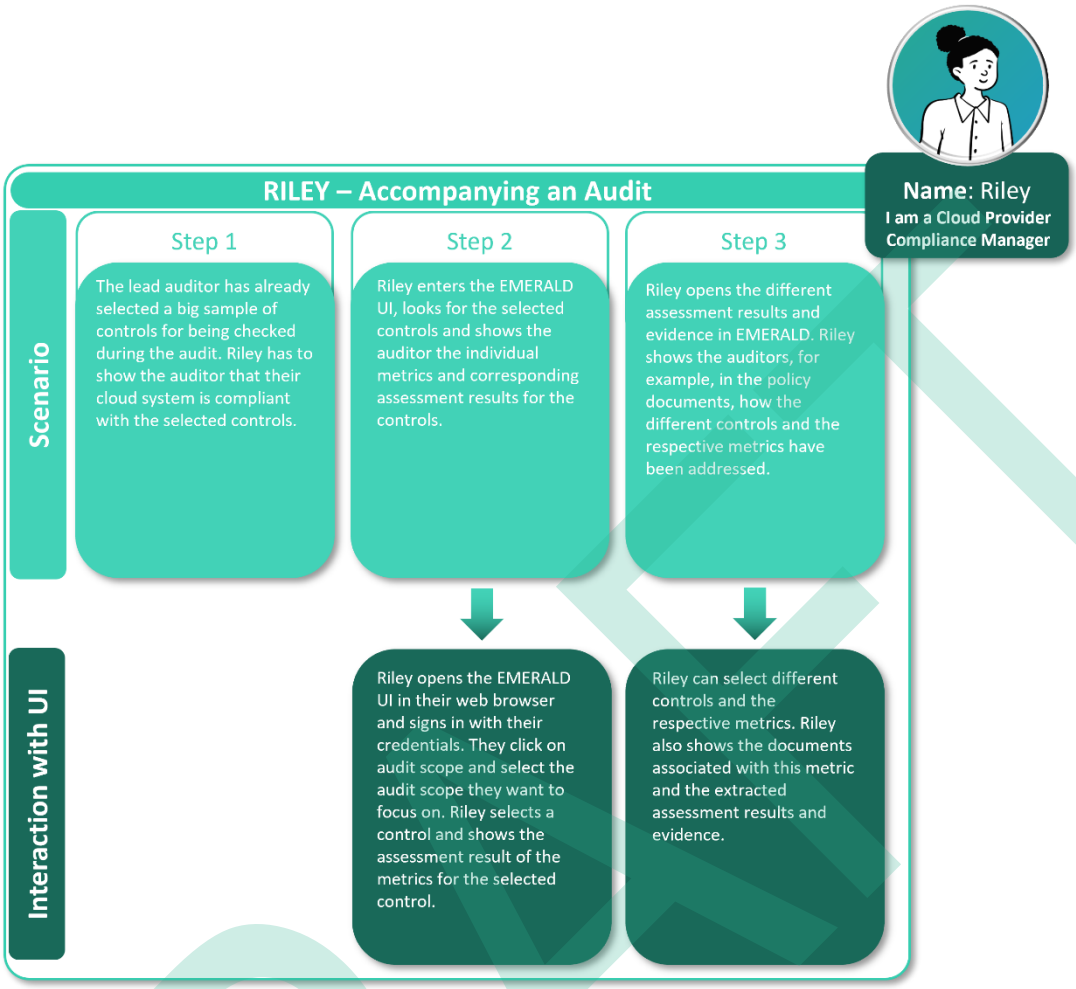

Figure 9. Riley – Accompanying an Audit

3.2.5 Emerson – Bring your own certification scheme (BYOCS)

The scenario "Bring your own certification scheme" for Emerson was divided into the following five steps, as depicted in Figure 10.

Step 1 – Scheme Information:

- **Emerson's Tasks**: 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.
- **Interaction with the EMERALD UI**: no interaction required.

Step 2 – Creating a Custom Certification Scheme:

- **Emerson's Tasks**: Emerson builds up a new certification scheme based on the combination of regulations that the institution needs to be compliant with, by creating a custom certification scheme. They select the set of controls from each available certification scheme and creates custom controls.
- **Interaction with the EMERALD UI**: Emerson opens the EMERALD UI in their web-browser and signs in with their credentials. They select the certification schemas tab, select the option of "create custom certification scheme", and name it. Then, Emerson selects a list of controls from different certification schemas and saves it.

Step 3 – Create an Audit Scope:

- **Emerson's Tasks**: Emerson creates an audit scope that will be used for managing cloud solutions and the respective standard.
- **Interaction with the EMERALD UI**: Emerson goes to the EMERALD tab for creating a new audit scope, selecting the previous created certification scheme and the respective target of evaluation.

Step 4 – Automatic Check:

- **Emerson's Tasks**: Emerson's task is now to go through all controls to check if all of them can be met with some evidence (technical or organisational).
- **Interaction with the EMERALD UI**: Emerson goes to EMERALD UI and visualizes the assessment results and evidence linked to the control and the overall compliance in a first automatic iteration.

Step 5 – Control Status Check:

- **Emerson's Tasks**: Emerson needs to check the status of the controls regarding the metrics, evidence, and states. Emerson uses different functionalities available in the EMERALD UI to filter controls and uses different visualisations of the overall status of all controls, etc., to find out which controls need some work, and which are already compliant.
- **Interaction with the EMERALD UI**: Emerson enters the EMERALD UI and visualizes, filters, and manages the controls.

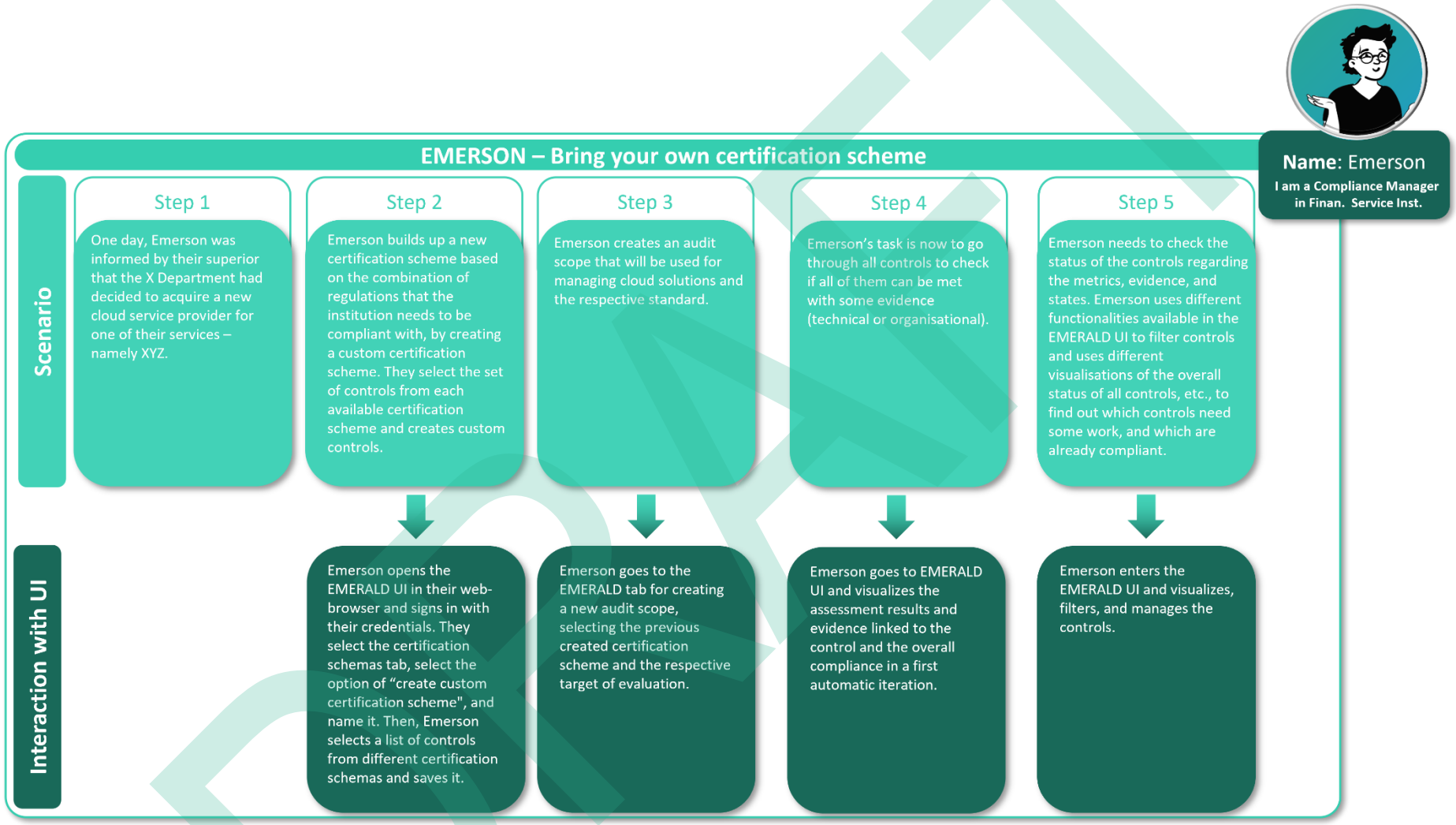

Figure 10. Emerson – Bring your own Certification Scheme

3.2.6 Dylan - Control Implementation

The scenario "Control Implementation" for Dylan was also divided into six steps, as depicted in Figure 11.

Step 1 – Checking Assigned Controls:

- **Dylan's Tasks**: Dylan opens the EMERALD UI to check if any newly assigned controls require action.
- **Dylan's Interaction with the EMERALD UI**: Dylan opens the EMERALD UI in their web browser, signs in using their credentials, and is redirected to the landing page, where all assigned controls are displayed.

Step 2 - Assigning Metrics to Controls:

- **Dylan's Tasks**: Dylan checks the controls assigned to them and whether appropriate metrics are already assigned to the control. If none are assigned or some are not suitable, Dylan updates the mapping by adding, removing, or replacing metrics as needed.
- **Dylan's Interaction with the EMERALD UI:** Dylan checks the control details, and if no metrics are assigned, they can navigate to the control in the metrics mapping (via the certification schemes menu). In the metrics mapping, they can select a set of metrics for the control.

Step 3 – Assigning Controls to a Colleague:

- **Dylan's Tasks**: If Dylan identifies an open control but cannot provide the required evidence, they assign it to their colleague Y.
- **Dylan's Interaction with the EMERALD UI**: In the detailed view of the control, Dylan assigns Y as the implementer.

Step 4 - Viewing Assigned Controls:

- **Y's Tasks:** Y reviews the newly assigned control and opens it to gather more details.
- **Y's Interaction with the EMERALD UI:** Y filters for the assigned controls in the audit scope and clicks on the control, which opens the detailed view of a control.

Step 5 – Reviewing Metrics Implementation Status:

- **Y's Tasks**: Y reviews all metrics for compliance and determines whether they can implement the control themselves or if it should be assigned to someone else.
- **Y's Interaction with the EMERALD UI**: Y can view the compliance status of the relevant metrics in the control detail's view. If the metrics are not yet implemented and Y cannot work on them, the control can be reassigned to another colleague, Z.

Step 6:

- **Z's Tasks**: Z implements the metrics for the assigned control and makes sure the evidence is included in the EMERALD solution.
- **Z's and Dylan's Interaction with the EMERALD UI**: Z reviews the list of metrics, implements each one, updates the required evidence, and confirms completion in EMERALD. Dylan is automatically notified of the updated control status, and the control workflow status reflects the new implementation progress.

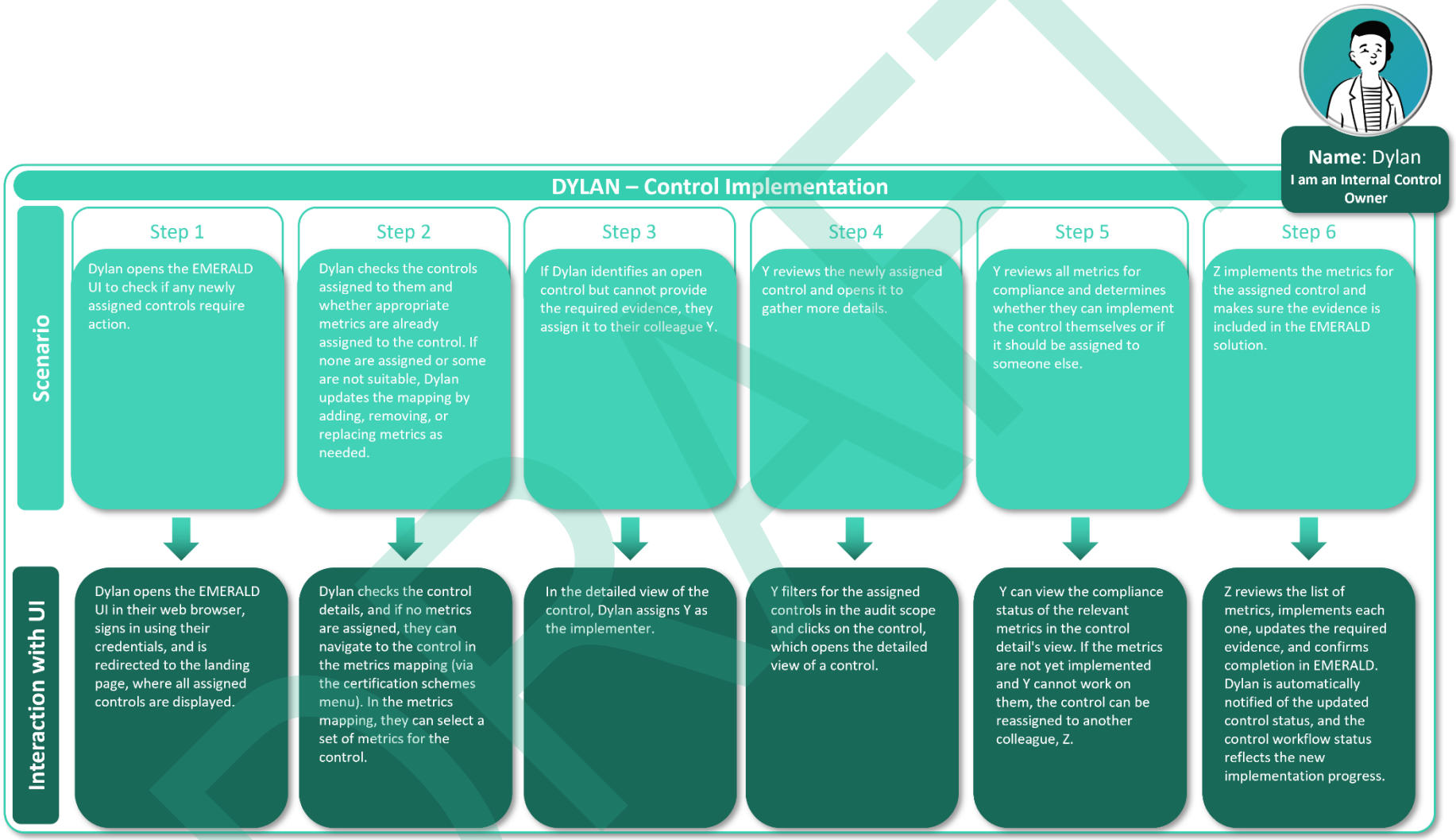

Figure 11. Dylan – Control Implementation

3.2.7 Morgan – Checking Metrics and Evidence

The scenario "Checking Metrics and Evidence" for Morgan was divided into four steps as depicted in Figure 12.

Step 1 – Checking Assigned Controls:

- **Morgan's Tasks**: Morgan logs into the EMERALD UI to check for any newly assigned controls. From the landing page, Morgan can immediately see if new controls have been assigned. By clicking on a control, Morgan is directed to the associated audit scope and can filter the list to focus on newly assigned controls that require action.
- **Morgan's Interaction with the EMERALD UI:** Morgan logs into the EMERALD UI, reviews the list of assigned controls on the landing page, clicks on a newly assigned control to open its audit scope, and applies filters to focus on controls that need attention.

Step 2 – Reviewing Target Metrics:

- **Morgan's Tasks**: Morgan opens the first newly assigned control and examines the related metrics. They review the status of each metric to gain insights and understand the overall compliance requirements.
- **Morgan's Interaction with the EMERALD UI**: Morgan opens the control within the EMERALD UI, reviews the associated metrics, and checks the details and status of each metric to gather insights.

Step 3 – Verifying Evidence:

- **Morgan's Tasks**: Morgan investigates the metric details, checking which other controls the metric is linked to, as well as reviewing the evidence extractors and any automatically provided evidence. In some cases, Morgan needs to adapt the required evidence (source code, policy documents) outside of the EMERALD UI.
- **Morgan's Interaction with the EMERALD UI**: Morgan opens a specific metric in the EMERALD UI, reviews its general information, examines the evidence extractors linked to the metric, and evaluates the automatically gathered evidence.

Step 4 – Confirming Implementation:

- **Morgan's Tasks**: If everything is correct, Morgan notifies the Compliance Manager that the control has been successfully implemented. If there are discrepancies, Morgan revisits specific metrics to troubleshoot and resolve issues.
- **Morgan's Interaction with the EMERALD UI**: Morgan updates the workflow status of the control to "Implemented," manually sets the compliance status to "Compliant" if necessary, and ensures that the Compliance Manager is automatically notified of the update.

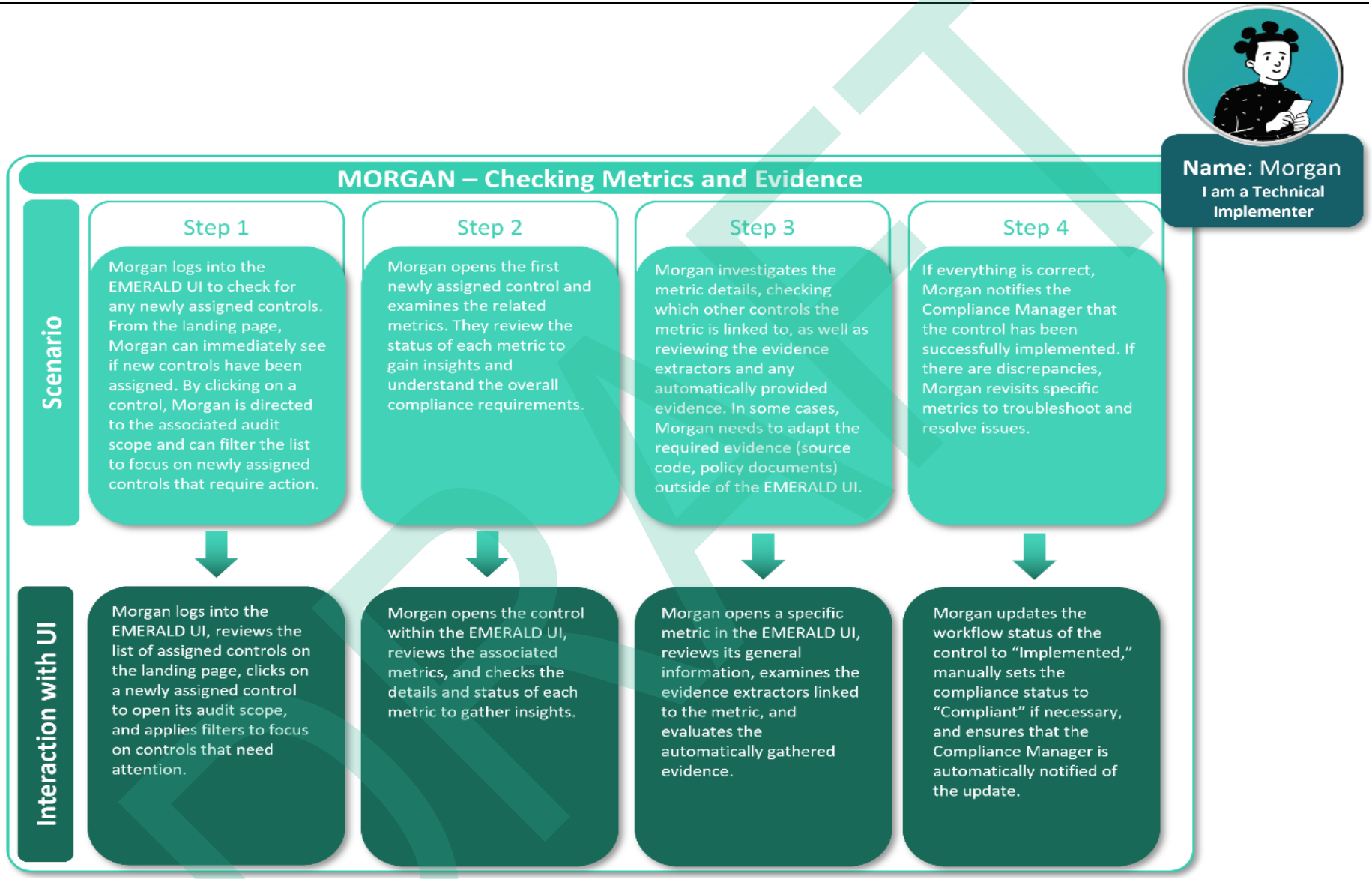

Figure 12. Morgan – Checking Metrics and Evidence

3.2.8 Charlie – Preparation of an audit by an internal auditor

The scenario "Preparation of an audit by an internal auditor" for Charlie was divided into five steps as depicted in Figure 13.

Step 1 – Logging into EMERALD UI:

- **Charlie's Tasks**: Charlie, an internal auditor, is responsible for managing audit processes against EUCS, including audit preparation. As part of the preparation, Charlie needs to review all controls and ensure that each one has the required evidence assigned for the relevant audit scopes.
- **Charlie's Interaction with the EMERALD UI:** Charlie opens the EMERALD UI in their web browser, signs in using their credentials, navigates to the audit scopes, and selects the specific scope they want to review.

Step 2 – Reviewing the current Status:

- **Charlie's Tasks**: Charlie reviews the workflow and compliance status within the selected audit scope by using the different views available in the overview tab.
- **Charlie's Interaction with the EMERALD UI**: Charlie navigates through the various views in the audit scope, uses the progress view to monitor the current workflow states, checks the compliance view to assess the compliance status of controls, and reviews a summarized snapshot of both statuses in the overall view.

Step 3 – Identifying Non-Compliant Controls:

- **Charlie's Tasks**: Charlie checks the non-compliant controls.
- **Charlie's Interaction with the EMERALD UI**: Charlie opens the compliance view and applies a filter to display only the controls that are noncompliant (marked with a red X).

Step 4 – Analysing the Causes of Non-Compliance:

- **Charlie's Tasks**: When Charlie discovers a non-compliant control, they analyse which metric is causing the non-compliance so they can provide accurate information to the compliance manager.
- **Charlie's Interaction with the EMERALD UI**: Charlie opens the detailed view of the control, investigates the non-compliant metrics, and reviews the related assessment result and evidence to identify the root cause, such as thresholds not being met, missing measurements due to connection issues, or untrustworthy evidence.

Step 5 – Creating a Report:

- **Charlie's Tasks**: After reviewing all non-compliances, Charlie prepares an internal report summarizing the findings for the compliance manager.
- **Charlie's Interaction with the EMERALD UI**: Charlie exports a detailed summary of all non-conformities, including supporting information, via the report tab in the EMERALD UI.

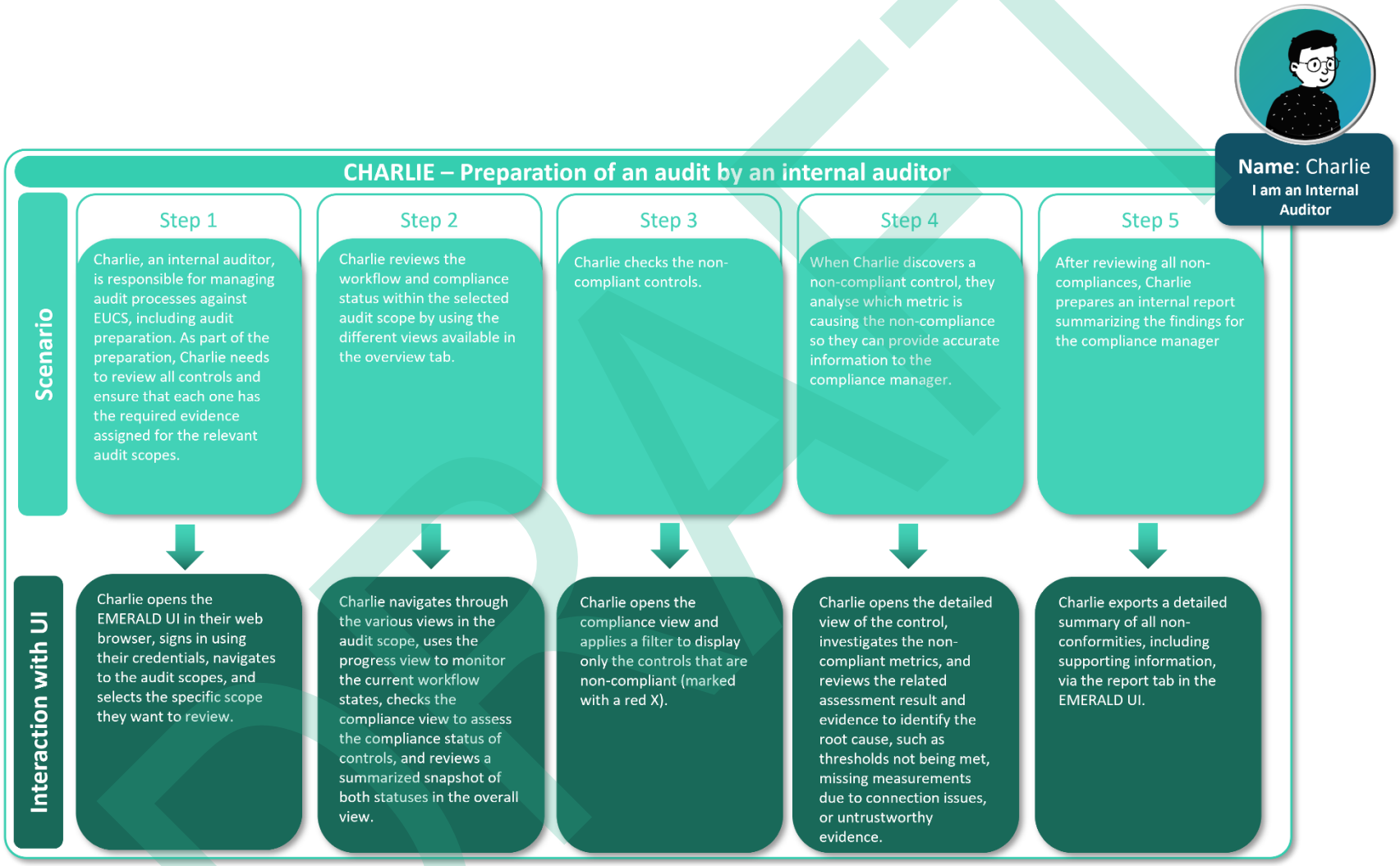

Figure 13. Charlie – Reparation of an Audit by an Internal Auditor

3.2.9 Jarkko – Scoping

The scenario "Scoping" for Jarkko was also divided into two steps, as depicted in Figure 14.

Step 1 – Documenting the Audit Scope:

- **Jarkko's Tasks**: Jarkko reviews the selected audit scope to understand its overall status, including the number of controls in different workflow and compliance states.
- **Jarkko's Interaction with the EMERALD UI**: From the landing page, Jarkko clicks on "Audit Scopes" and reviews the information of the relevant audit scope.

Step 2 – Investigating Non-Compliant Controls:

- **Jarkko's Tasks:** Jarkko investigates specific controls to identify the causes of non-compliance, such as missing metrics, thresholds not met, or connection issues.
- **Jarkko's Interaction with the EMERALD UI:** Jarkko opens the detailed view of a non-compliant control to review its associated metrics, assessment results and evidence, allowing them to pinpoint the reason for non-compliance.

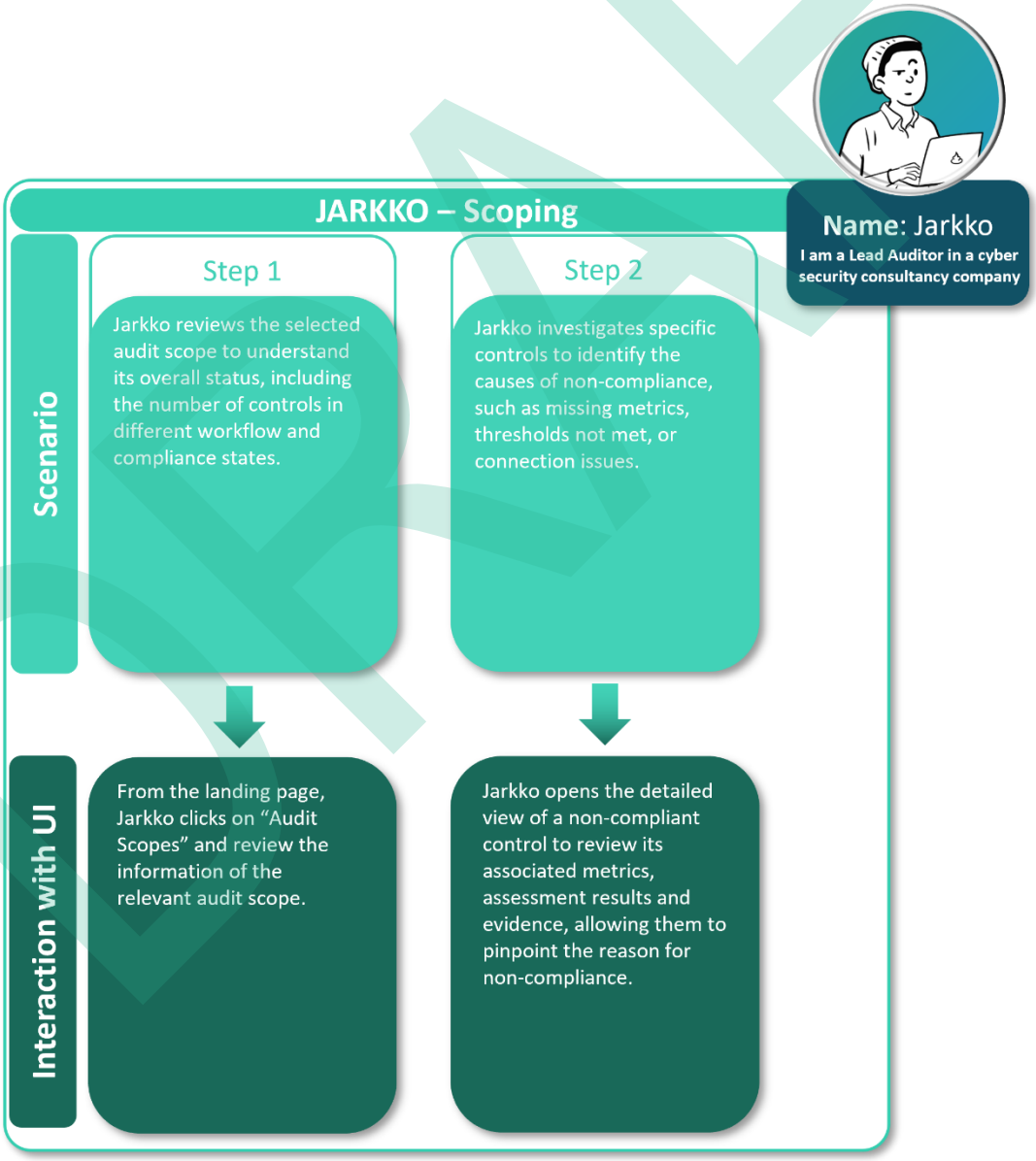

Figure 14. Jarkko - Scoping

3.2.10 Jarkko – Preparing for Audit

The scenario “Preparing for Audit” for Jarkko was also divided into four steps, as depicted in Figure 15.

Step 1 – Accessing the EMERALD Project:

- **Jarkko’s Tasks**: Jarkko and the auditor team need to be assigned to the existing EMERALD project.
- **Jarkko’s Interaction with the EMERALD UI**: Jarkko opens the EMERALD UI in their web browser, signs in using their credentials, and verifies access to the relevant audit scope.

Step 2 – Reviewing the Audit Scope:

- **Jarkko’s Tasks**: Jarkko needs to review the scope of the audit to understand its coverage and focus areas.
- **Jarkko’s Interaction with the EMERALD UI**: Jarkko navigates to the audit scope section, clicks on it, and selects the specific scope they want to review.

Step 3 – Verifying the Self-Assessment Questionnaire [only relevant for EUCS]:

- **Jarkko’s Tasks:** Jarkko and the auditor team need to check the answers to the self-assessment questionnaire, if applicable (for EUCS only). They note any missing or incorrect responses for further actions.
- **Jarkko’s Interaction with the EMERALD UI:** Jarkko navigates to the "Questionnaire“ tab, reviews the pre-filled answers, and verifies completeness. They can enter their comments in the “Non-conformities of the control” field, strictly reserved for auditors only.

Step 4 – Reviewing Metrics:

- **Jarkko’s Tasks**: Jarkko and the auditor team need to check the metrics assigned to a control and the corresponding target values of the metrics.
- **Jarkko’s Interaction with the EMERALD UI:** Jarkko selects a control and clicks on it to see the metrics assigned for the selected control. Here, they get an overview of the assessment results for the associated metrics of the selected control.

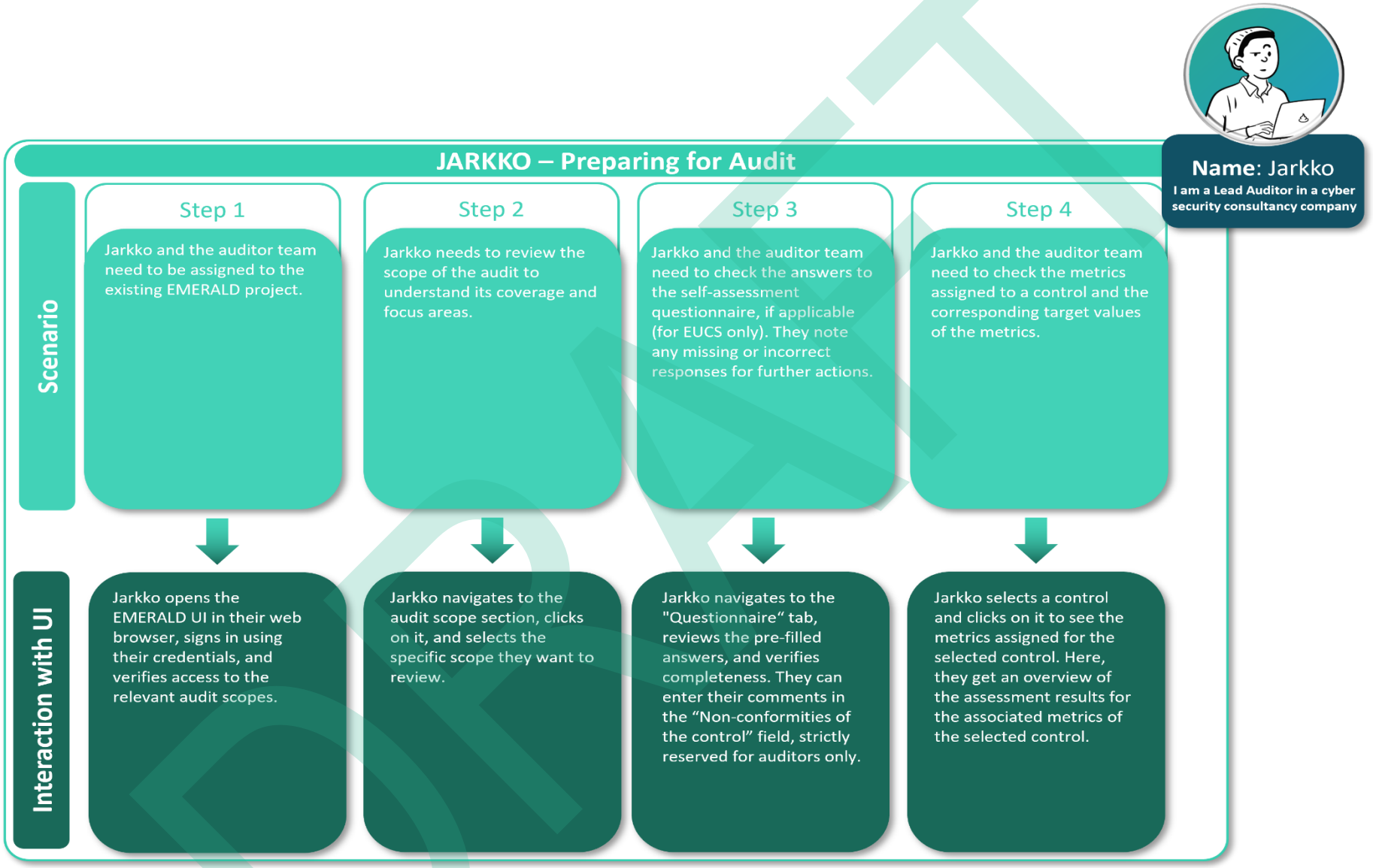

Figure 15. Jarkko – Preparing for Audit

3.2.11 Jarkko – Organisational Audit

The scenario "Organisational Audit" for Jarkko was divided into four steps, as depicted in Figure 16.

Step 1 – Checking Integrity and Validity of Results:

- **Jarkko's Tasks:** Jarkko needs to ensure the audit data is accurate and reliable. EMERALD was used to support this process.
- **Jarkko's Interaction with the EMERALD UI:** Jarkko opens the EMERALD UI in their web browser and signs in using their credentials.

Step 2 – Verifying Document Updates:

- **Jarkko's Tasks:** Jarkko checks whether policy documents are updated regularly to ensure compliance with the latest requirements.
- **Jarkko's Interaction with the EMERALD UI:** In the Target of Evaluation screen, under the document tab, Jarkko views the last upload date for each policy document.

Step 3 – Accessing Non-Compliant or Pending Controls:

- **Jarkko's Tasks:** Jarkko reviews the results of controls that are non-compliant or pending to analyse potential risks.
- **Jarkko's Interaction with the EMERALD UI:** Jarkko navigates to the audit scopes, selects the relevant scope, and uses the compliance view to filter for controls that are marked as non-compliant or still pending.

Step 4 – Adding Notes for the Audit Report:

- **Jarkko's Tasks:** Jarkko documents findings and observations by adding notes that will be included in the audit report.
- **Jarkko's Interaction with the EMERALD UI:** Jarkko navigates to the report submenu and clicks on create snapshot. The report will be automatically downloaded and in the downloaded document, they can enter general notes to be included into the final report.

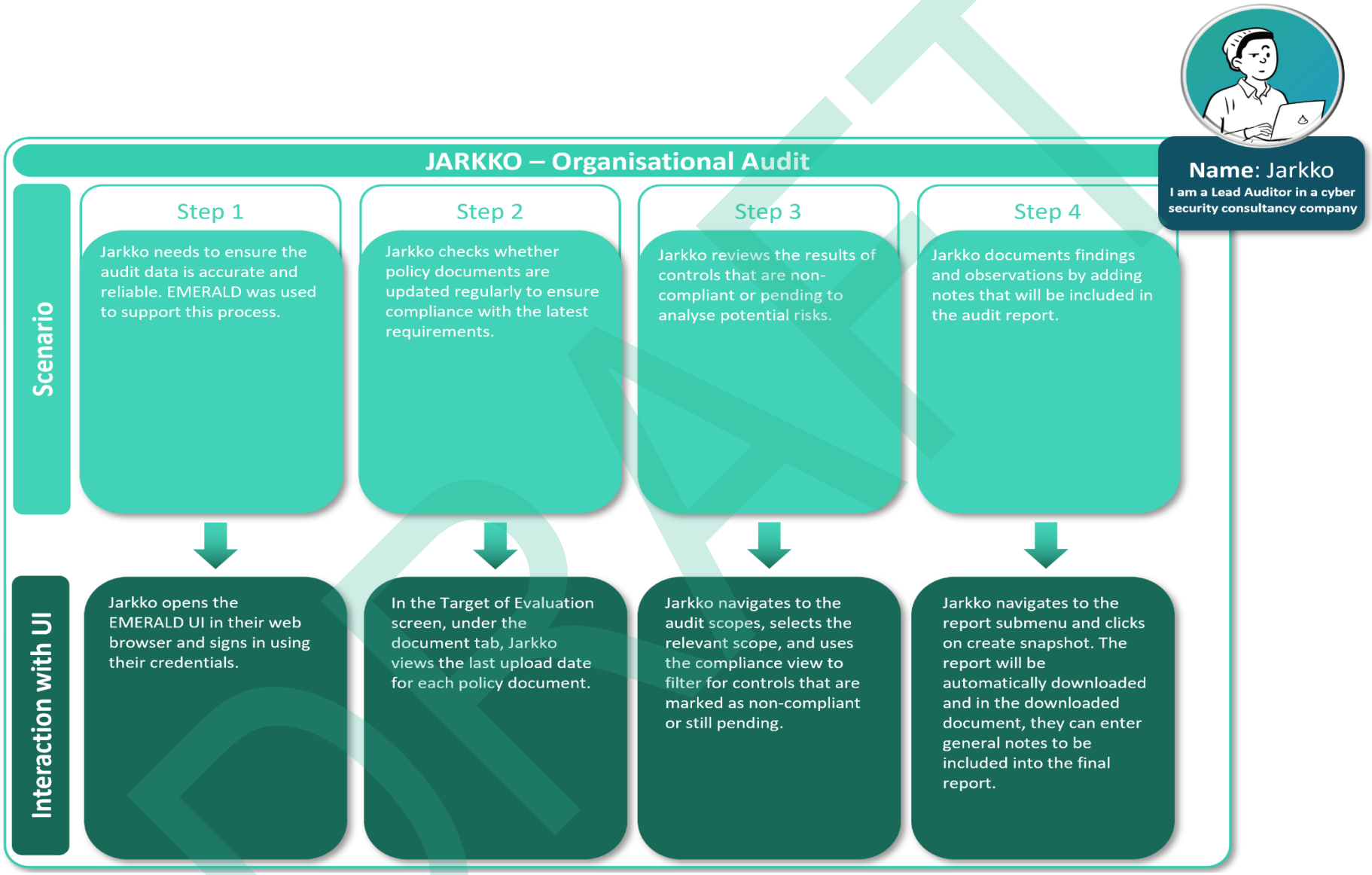

Figure 16. Jarkko – Organisational Audit

3.2.12 Jarkko – Certification

The scenario "Certification" for Jarkko was also divided into three steps, as depicted in Figure 17.

Step 1 – Identifying Non-Compliances:

- **Jarkko's Tasks:** Jarkko identifies all controls that are non-compliant within the selected audit scope.
- **Jarkko's Interaction with the EMERALD UI:** Jarkko opens the EMERALD UI in their web browser, signs in with their credentials, and navigates to the audit scopes section to open the relevant audit scope, and filters for all non-compliant controls.

Step 2 – Creating and Sharing the Audit Report:

- **Jarkko's Tasks**: Jarkko creates an audit report and translates the identified non-compliances into documented findings, which are then communicated to relevant stakeholders.
- **Jarkko's Interaction with the EMERALD UI:** In the submenu report in the track record of evidence view, Jarkko navigates to the compliance proof section, where the compliance status for each control is summarized. Jarkko downloads the Report.

Step 3 – Preparing the Annex with Scope Details:

- **Jarkko's Tasks:** Jarkko is responsible for preparing an annex to the audit report that clearly documents the scope. This annex should provide full transparency by distinguishing between evaluated controls and metrics versus those not evaluated.
- **Jarkko's Interaction with the EMERALD UI:** While in the track record of evidence view, Jarkko accesses the statement of applicability, which summarizes any deviations from the audit scope by category. This information can also be downloaded separately using the download report option.

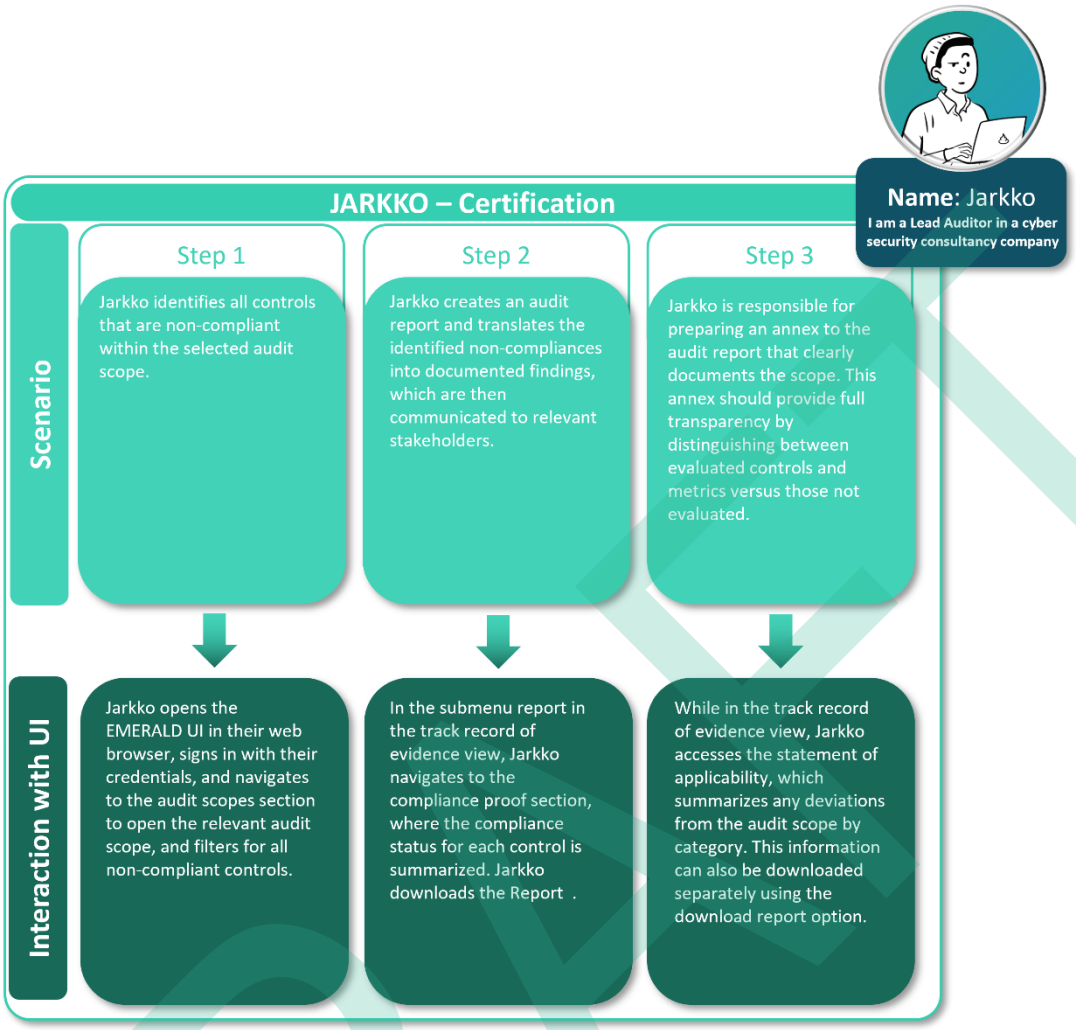

Figure 17. Jarkko - Certification

3.2.13 Eero – Technical Audit

The scenario "Technical Audit" for Eero was also divided into six steps, as depicted in Figure 18.

Step 1 – Log In and Verify Access:

- **Eero's Tasks**: Eero needs to ensure that the tools and results used in the audit are valid and reliable. EMERALD was used to support this process, therefore Eero needs to log into the EMERALD UI.
- **Eero's Interaction with the EMERALD UI**: Eero opens the EMERALD UI in their web browser and signs in using their credentials.

Step 2 – Review Technical Evidence Updates:

- **Eero's Tasks**: Eero needs to verify that technical evidence is updated regularly.
- **Eero's Interaction with the EMERALD UI**: Eero navigates to the respective audit scope and selects the relevant scope. For each relevant control, they review the control details to see the last update date of the assessment result and evidence for each metric.

Step 3 – Access Non-Compliant Control Results:

- **Eero's Tasks:** Eero accesses the results of the controls that are non-compliant or pending.
- **Eero's Interaction with the EMERALD UI:** Eero clicks on audit scope and selects the audit scope they want to focus on. They filter in the control list for non-compliant controls.

Step 4 – Conduct Technical Analysis:

- **Eero's Tasks**: Eero needs to do a technical analysis with tools and manual methods.
- **Eero's Interaction with the EMERALD UI:** Not supported in the EMERALD UI.

Step 5 – Add Notes for the Audit Report:

- **Eero's Tasks**: They add information (notes) for the report of the audit.
- **Eero's Interaction with the EMERALD UI**: Eero navigates to the report menu and clicks on create report to download it. Any additional information and notes can be added in the downloaded document.

Step 6 - Communicate Findings:

- **Eero's Tasks**: Eero communicates with compliance managers, technical experts of the CSP/customer, the lead auditor.
- **Eero's Interaction with the EMERALD UI**: This communication will happen outside of the EMERALD UI.

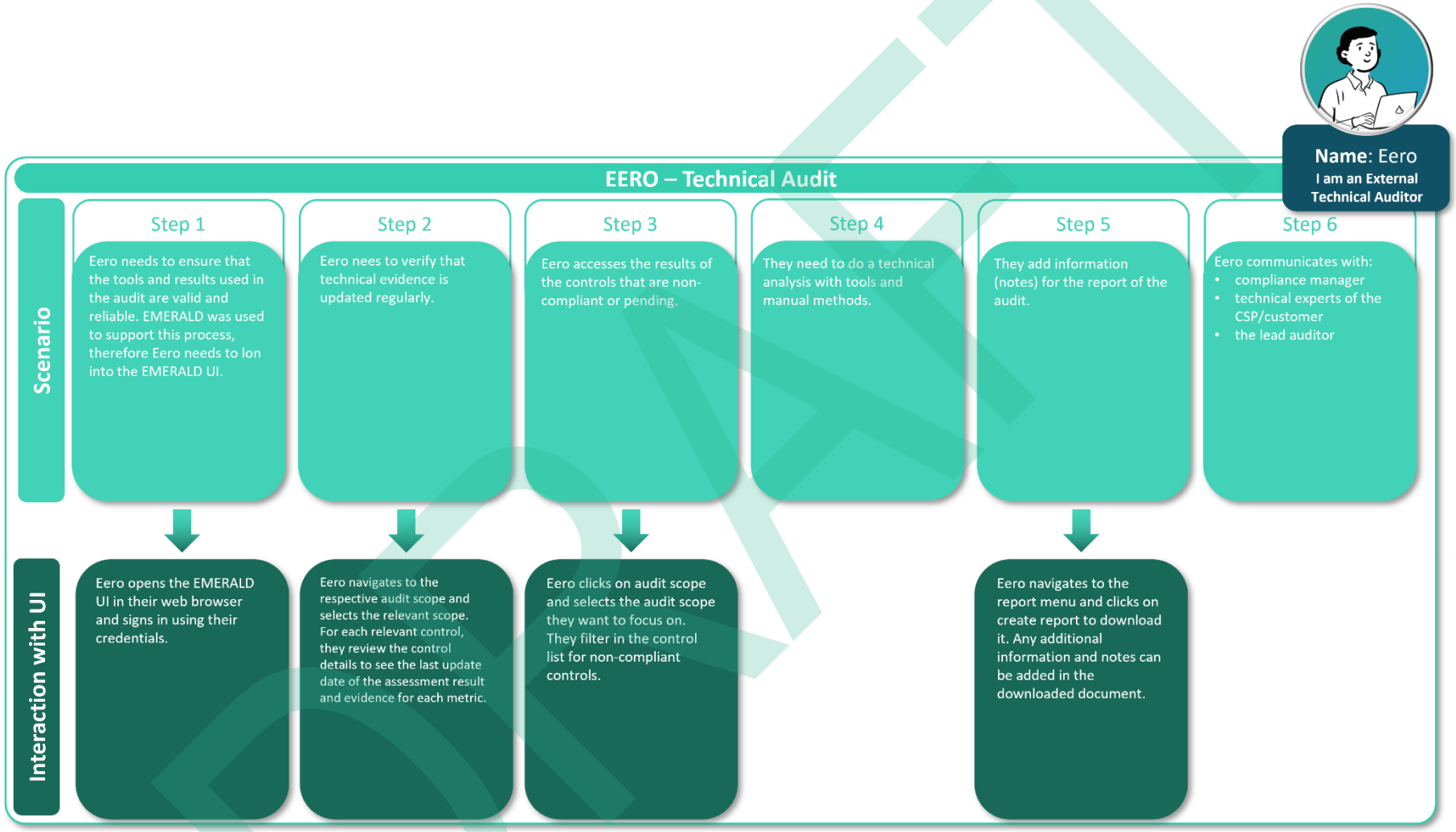

Figure 18. Eero – Technical Audit

3.2.14 Eero – Reporting

The scenario "Reporting" for Eero was also divided into four steps, as depicted in Figure 19.

Step 1 – Logging in:

- **Eero's Tasks**: Eero needs to provide technical information to the lead auditor, so it can be included in the final report. The audit preparation tool used was EMERALD. Therefore, they can gather insights from the EMERALD UI.
- **Eero's Interaction with the EMERALD UI**: Eero opens the EMERALD UI in their web browser and signs in with their credentials.

Step 2 – Identify Non-Compliance:

- **Eero's Tasks**: Eero needs to identify all non-compliant controls.
- **Eero's Interaction with the EMERALD UI**: Eero clicks on audit scopes section and selects the audit scope they want to focus on. They filter in the control list for controls that are non-compliant.

Step 3 – Generate Audit Report:

- **Eero's Tasks:** Eero prepares an audit report and includes additional technical details to provide further clarification to the lead auditor on the non-compliance.
- **Eero's Interaction with the EMERALD UI**: Eero navigates to the report menu and clicks on create report to download it. Any additional information and notes can be added in the downloaded document.

Step 4 – Communicate Findings:

- **Eero's Tasks**: Eero communicates the findings to the lead auditor.
- **Eero's Interaction with the EMERALD UI:** This will not be supported in EMERALD.

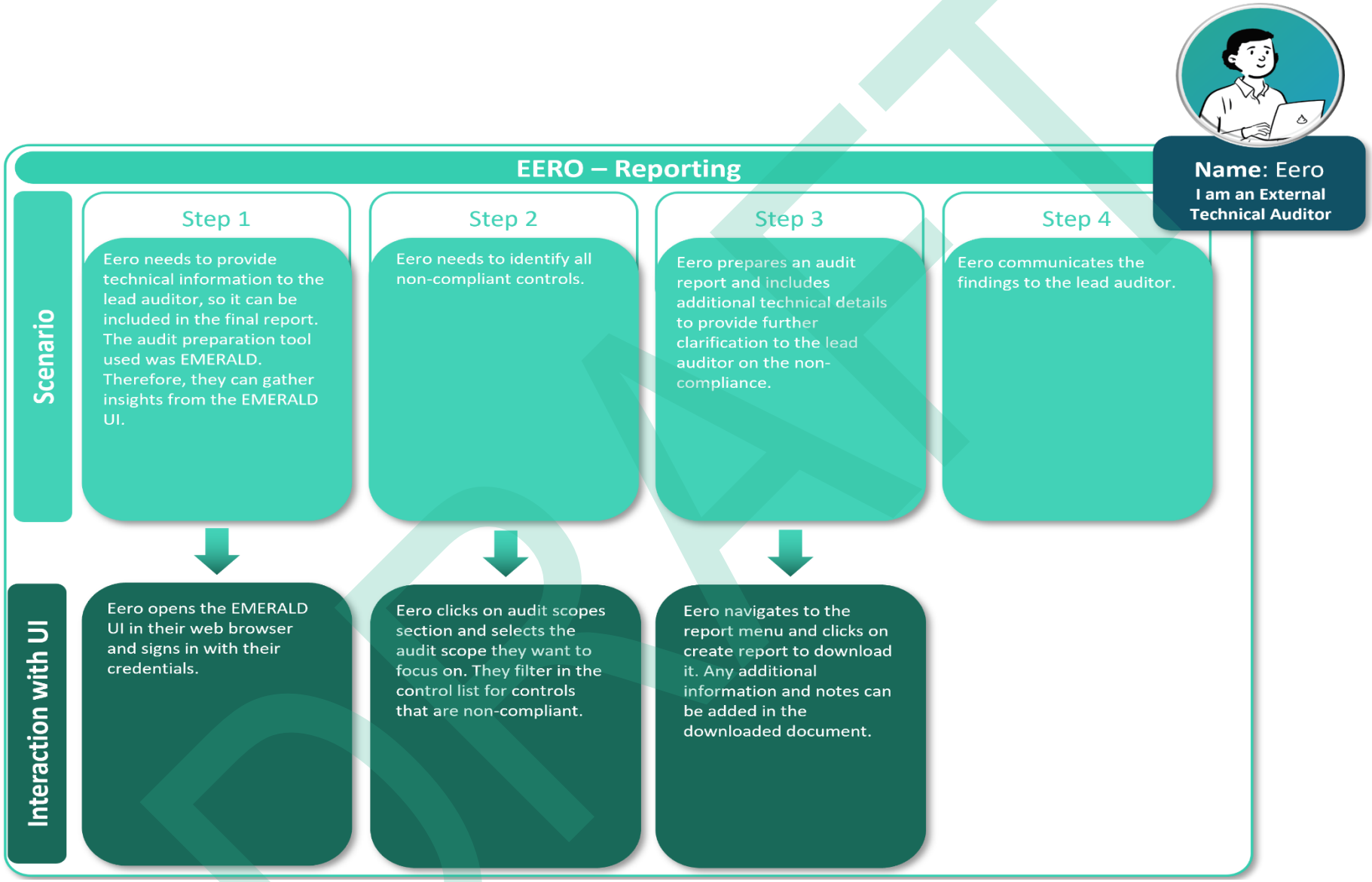

Figure 19. Eero – Reporting

4 Clickable Mock-up

The overall EMERALD UI should provide 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."* as described in the DoA [2]. Therefore, in WP4 several activities with pilot partners as well as component owners were conducted to elicit the needs of the different partners (as described in Sections 2.1, 2.2, 2.3, and 2.4).

From these activities, we were able to derive three major visualisation streams and some sub-visualisation streams so that the EMERALD UI can support all relevant stages during an audit: Stream 1: Setting up and managing the Certification Target; Stream 2: Setting up and managing the Audit Scope; Stream 3: Setting up and managing the certification schemes. Additional visualisations include metrics management, user management, and the self-assessment questionnaire. An overview of the EMERALD UI, the different visualisation streams, and the related EMERALD components is presented in Figure 20.

The different workshops which we have conducted with the individual component owners that we have presented in D4.3 [1] have been added to the Appendix to be complete. In this section we focus on the presentation of all functionalities which we have implemented in the clickable mock-up. We present in detail the three main visualisation streams and we also present additional available functionality of the UI.

- **Stream 1: Setting up and managing certification schemes**: This stream focuses on the upload of the certification schemes, the possibility to browse through them as well as to do the mapping of controls and metrics, and the mapping of controls to controls across different schemes. Additionally, it offers the possibility to create a scheme of your own and to download certification schemes. This stream is presented in Section 4.3 also shortly describing the interplay of *RCM* and the *MARI* components in the EMERALD UI.
- **Stream 2: Setting up and managing the targets of evaluation**: This stream focusses on the selection of the targets of certification (e.g. cloud services,...), allows to select and setup the different evidence extractors including *eknows-e3, Codyze, AI-SEC, Clouditor Discovery*, and *AMOE*, allows to enable/disable the TWS, and to manage the access rights for each target of evaluation. This stream will be presented in Section 4.4.
- **Stream 3: Setting up and managing audit scopes**: This stream focuses on setting up the audit scopes, thus selecting the target of certification and the corresponding certification scheme. Furthermore, it shows the assessment results of the evidence extractors and allows to manage all controls regarding their compliance or non-compliance (e.g. *AMOE, Clouditor-Orchestrator*); additionally different controls can be assigned to different people and departments. If dealing with EUCS as certification scheme, a self-assessment questionnaire can be created. And different reports are available. This stream will be presented in the Section 4.5.
- **Additional Functionality**: First, there is an overview page for the different self-assessment questionnaires that have been created for different audit scopes, which is presented in Section 4.7. Second, there is a view that allows to navigate the available metrics per metrics category and their assignment to controls in the different audit scopes presented in Section 4.6. Finally, there exists the possibility to invite new users, and to manage the users' roles presented in Section 4.8.

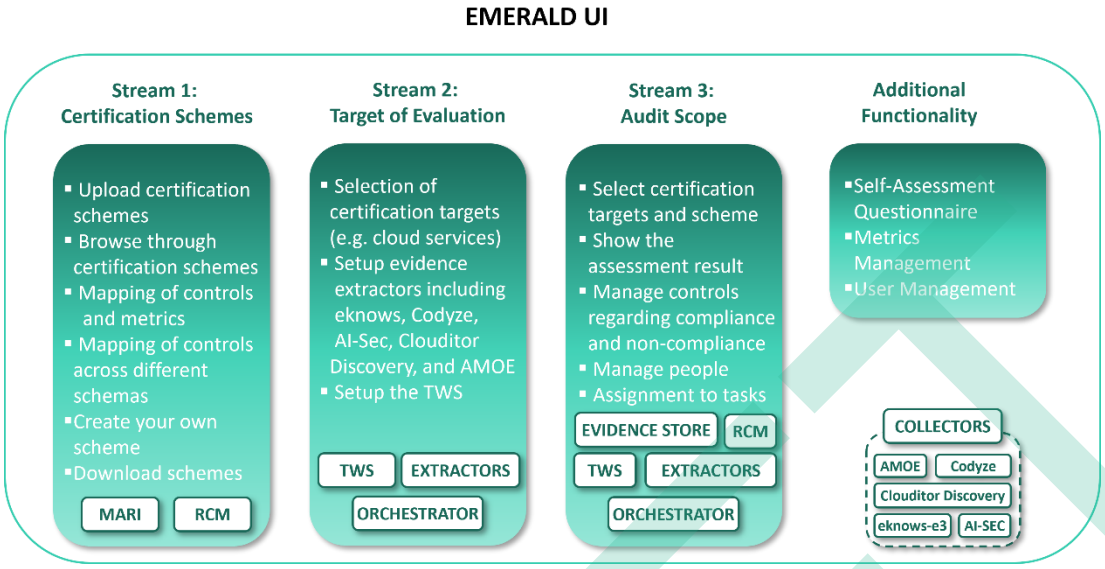

Figure 20. Overview of the EMERALD UI Visualisation Streams

4.1 Access Rights for the EMERALD UI per Persona

Before we start with presenting the clickable mock-up, we will first describe the access rights for the different user roles. The development of the personas, their characteristics, their tasks in their working environment, as well as how EMERALD might support them, is used to clearly define the access rights in the EMERALD UI. Based on the respective roles, an EMERALD user has more or less access to the individual EMERALD UI parts. For example, while a compliance manager (CM) is allowed to create, view, edit, and delete a self-created target of evaluation, an auditor gets only read access for the target of evaluation.

In the following, we present for all major EMERALD UI parts the concrete access rights per persona:

- Access rights for the certification schemes are presented in Table 7
- Access rights for the targets of evaluation are presented in Table 8
- Access rights for the audit scopes are presented in Table 9
- Access rights for the metrics management are presented in Table 10
- Access rights for the user management are presented in Table 11

During the development of the EMERALD UI and after having completed all persona, scenario, and user journey workshops, one persona turned out to be missing: namely, the Chief Information Security Officer (CISO). The CISO is a role relevant in the compliance as a service process for FABA, so we added this role in the access rights descriptions. Furthermore, we also added the administrator role for completeness.

Table 7. Access Rights for all Personas towards the Certification Schemes

	Roles						
ACCESS RIGHTS PER ROLE	Compliance Manager	Expert Compliance Manager	Internal Control Owner	Technical Implementer	Auditors (internal & external)	Chief Information Security Officer	Admin
Certification Schemes							
• View certification schemes	X	X	X	X	X	X	X
○ View mapping of metrics to controls	X	X	X	X	X	X	X
○ View mapping of controls to controls across schemes	X	X	X	X		X	X
• Edit certification schemes:	X	X				X	X
○ Map metrics to controls	X	X				X	X
○ Map controls to controls across schemes	X	X				X	X
○ Add implementation guidelines		X					X
• Set values for metrics	X	X	X			X	X
• Download existing certification schemes	X	X				X	X
• Create new certification schemes		X					X
• Upload new certification schemes		X					X
• Delete a certification scheme		X					X

Table 8. Access Rights for all Personas towards the Targets of Evaluation.

	Roles						
ACCESS RIGHTS PER ROLE	Compliance Manager	Expert Compliance Manager	Internal Control Owner	Technical Implementer	Auditors (internal & external)	Chief Information Security Officer	Admin
Target of Evaluation							
• Create new ToE	X	X				X	X
• View assigned ToEs	X	X	X	X	X	X	X
• View all ToEs		X				X	X
• Edit ToEs	X	X	X	X		X	X
○ Upload new policy documents	X	X	X	X		X	X
○ Check resources	X	X		X		X	X
○ Adapt evidence extractor status	X	X		X		X	X
○ Enable and disable the trustworthiness system (TWS)	X	X				X	X
○ Upload information of AI-SEC sources	X	X	X	X		X	X
• Delete self-created ToE	X	X				X	X
• Delete all ToEs		X				X	X
• Manage the access rights of the self-created ToE	X	X				X	X
• Manage certifications	X	X				X	X

Table 9. Access rights for all personas towards the audit scopes.

	Roles						
ACCESS RIGHTS PER ROLE	Compliance Manager	Expert Compliance Manager	Internal Control Owner	Technical Implementer	Auditors (internal & external)	Chief Information Security Officer	Admin
Audit Scope							
• Create a new audit scope, but only for self-created ToEs	X	X				X	X
• Deleted only a self-created Audit Scope	X	X				X	X
• Edit an Audit Scope	X	X				X	X
○ Edit name	X	X				X	X
○ Change audit scope status (Setup, Internal Review, External Review, Continuous Compliance Management, Fixed).	X	X				X	X
○ Edit the assessment period	X	X				X	X
• Manage access rights	X	X				X	X
• Adapt the audit scope selection of metrics	X	X	X	X		X	X
• View all controls, assessment results, and metrics	X	X	X	X	X	X	X
• Edit all controls, assessment results, and metrics	X	X	X	X		X	X
○ Edit the workflow status of a control (open, in progress, implemented, ready for review)	X	X	X	X		X	X
○ Edit the workflow status of a control (set to accepted)		X				X	X
○ Change the owner of a control	X	X	X	X		X	X
○ Set a control manually to compliant	X	X	X	X		X	X
○ upload files and add comments, if a control cannot be assessed automatically	X	X	X	X		X	X
○ Edit the target value of a metric	X	X	X	X		X	X
○ Edit metrics applicability for a control	X	X	X	X		X	X

• Create and edit the Self-Assessment Questionnaire if the certification scheme is EUCS (except the field: "non-conformities of the requirement")	X	X	X	X		X	X
• View the Self-Assessment Questionnaire if the certification scheme is EUCS					X		X
○ Edit the field “non-conformities of the requirement”					X		X
• View and download reports	X	X	X		X	X	X
• Check why the integrity check of the TWS fails	X	X	X	X	X	X	X
• View notifications related to the audit scope	X	X	X			X	X

Table 10. Access rights for all Personas towards the Metrics Management

	Roles						
ACCESS RIGHTS PER ROLE	Compliance Manager	Expert Compliance Manager	Internal Control Owner	Technical Implementer	Auditors (internal & external)	Chief Information Security Officer	Admin
Metric Management							
• View all metrics categories and metrics	X	X	X	X		X	X
• View the related audit scopes (they created, they have access to)	X	X	X	X		X	X
• View for an audit scope (they created, they have access to) to which controls the metrics have been assigned to	X	X	X	X		X	X

Table 11. Access Rights for all Personas towards the User Management

ACCESS RIGHTS PER ROLE	Roles						
	Compliance Manager	Expert Compliance Manager	Internal Control Owner	Technical Implementer	Auditors (internal & external)	Chief Information Security Officer	Admin
User Management							
• Invite new users to EMERALD instance	X	X				X	X
• Assign role to users	X	X				X	X
• Change role of a user	X	X				X	X
• Delete a user	X	X				X	X

4.2 Landing Page

Figure 21 presents the landing page of the EMERALD UI. In the following, we describe the overall functionality of the landing page:

On the left side of Figure 21, the UI presents the overall navigation:

- Point 1: This is currently active, as the user is on the landing page (“Home”)
- Point 2: Go to the setup and management of the certification schemes
- Point 3: Go to the setup and management of the targets of evaluation
- Point 4: Go to the setup and management of the audit scopes
- Point 5: Go to the metrics management
- Point 6: Go to the self-assessment questionnaire
- Point 7: Go to the user management
- Point 8: Go to the glossary

On the right side of Figure 21, a user sees a current overview of the selected audit scope.

- Point 9: Shows the currently selected audit scope (“Audit Scope 1”). By using the dropdown menu, a user can switch to another audit scope.
- Point 10: Gives an overview of the current audit scope including the target of evaluation, the certification scheme, and the overall audit scope status.
- Point 11: By clicking on “Open audit scope” the user enters the currently selected audit scope.
- Point 12: Provides an overview of the controls’ status progress towards their implementation
- Point 13: Provides an overview of the compliance status of the current target of evaluation.
- Point 14: Shows the last activities that have been done in the audit scope, for example who was working on which control.
- Point 15: By clicking on the bell, the current list of notifications is shown. The yellow point on the bell shows, that there have been new notifications since the last visit for the current audit scope.
- Point 16: Here the currently logged in username and role is presented.

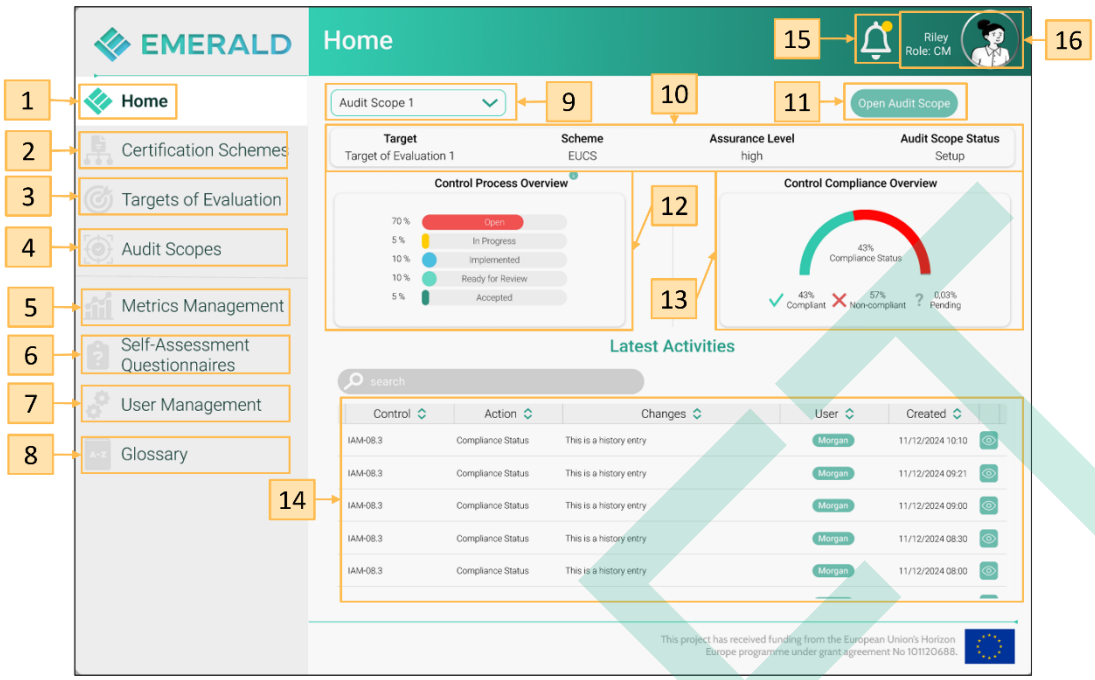

Figure 21. Landing Page of the EMERALD UI

4.3 Setup and Manage Certification Schemes

Stream 1: Setting up and managing certification schemes focuses on the management of the certification schemes. It offers the possibility to browse through existing certification schemes (Figure 23 point 1), it allows to do the mapping of controls and metrics (Figure 23 point 4) as well as to do the mapping of controls to controls across schemes. It offers the possibility to create a scheme of your own (Figure 23 point 3) by using controls of existing schemes or by defining new controls. Finally, it allows to upload and to download certification schemes (Figure 23 point 2). Figure 22 presents an overview of what a user is able to do in the certification scheme visualisation stream.

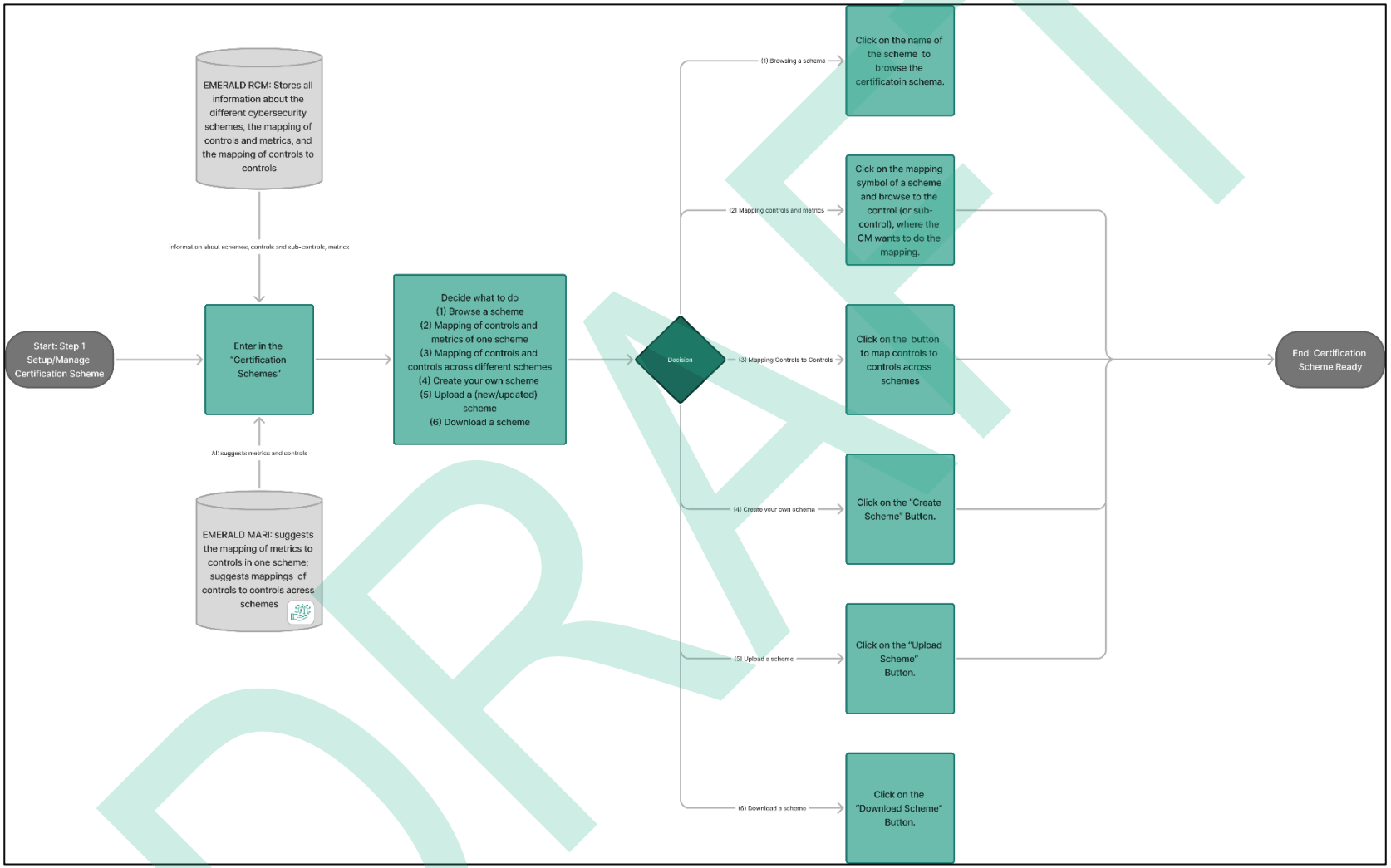

Figure 22. Overall Certification Scheme Process in the EMERALD UI

When entering the certification scheme section (Figure 21, point 2) in the EMERALD UI, the list of available certification schemes is presented as shown in Figure 23. Figure 23, point 1 shows the list of available certification schemes. For each scheme, the list presents the version number and the date and time, when it was uploaded. Additionally, a user (depending on the rights) and access the scheme by clicking on the name, access the mapping of controls and metrics, or delete the scheme.

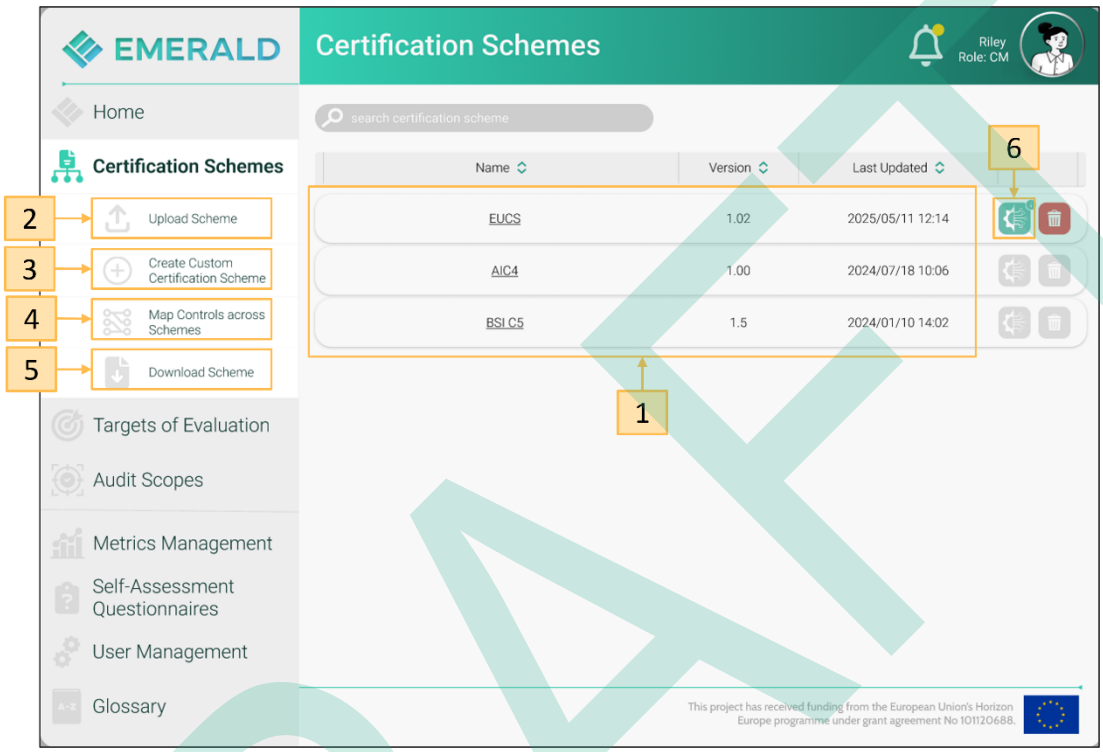

Figure 23. Certification Scheme – Overview

4.3.1 Browse Certification Schemes

By clicking on the name of a certification scheme like EUCS, the user is guided to Figure 24. Each scheme is presented and browsable in a hierarchical way. On top the categories are presented, when open the category or the sub-ordinated controls are shown like for EUCS (Figure 24, point 1). For each category or sub-ordinated control, the ID, the name, and a description is presented. When clicking on a sub-ordinated control for EUCS (or on a category in BSI C5) the different controls are presented as shown in Figure 25.

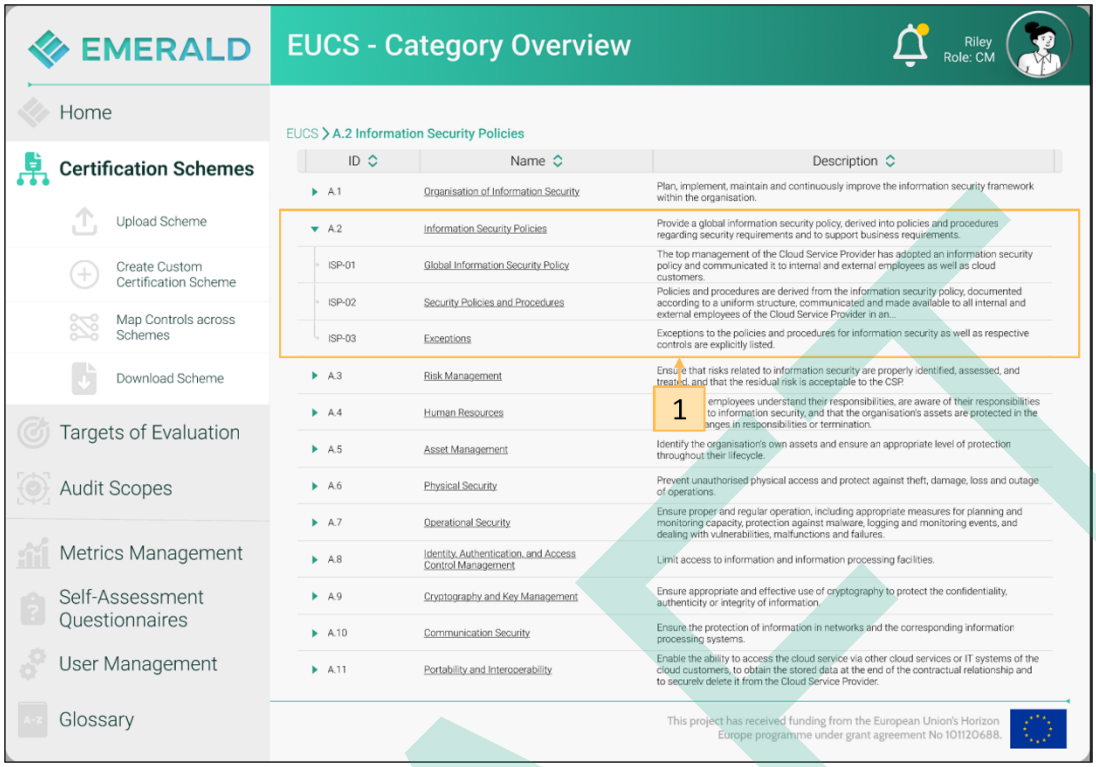

Figure 24. Certification Scheme – Browse Scheme - Categories

Figure 25 presents the list of controls related to a category and sub-ordinated control. For each control the ID is shown, the description, for EUCS the assurance level and the metrics that have been assigned to it (point 1). If a guideline for a control has been provided, a green button is available (point 2 in Figure 25) (grey = no guideline has been added, and green with a plus = add a new guideline).

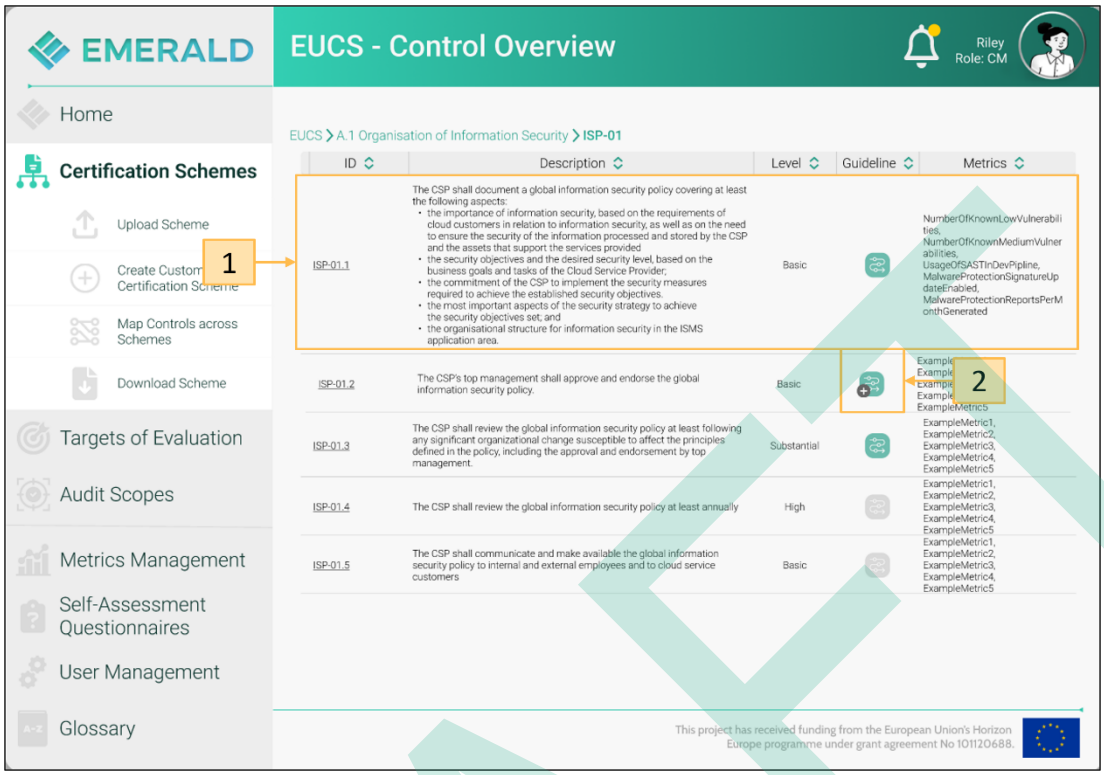

Figure 25. Certification Scheme – Browse Scheme - Controls

When clicking on the name of a control like for example “ISP-01.1”, more information about the control is presented as shown in Figure 26, point 1 allows to switch between different types of information. Figure 26Figure 26. Certification Scheme – Browse Scheme – Control Information, point 2 shows the description of the control; and when the scheme is EUCS, the assurance level of the control is presented.

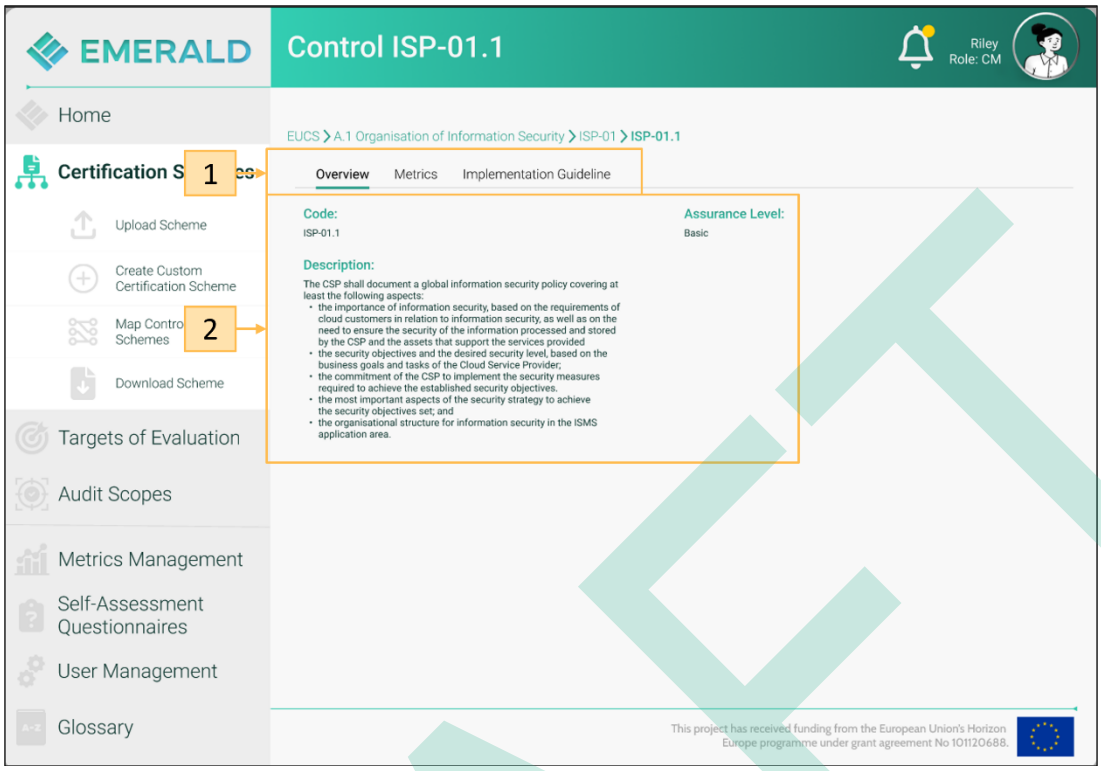

Figure 26. Certification Scheme – Browse Scheme – Control Information

Switching to the next tab "Metrics" provides the currently associated metrics to the control as presented in Figure 27. For each metric that is currently assigned to a control, the metric ID, the metric category, and the metric description are listed. The last column shows additionally to which other controls a metrics is assigned to.

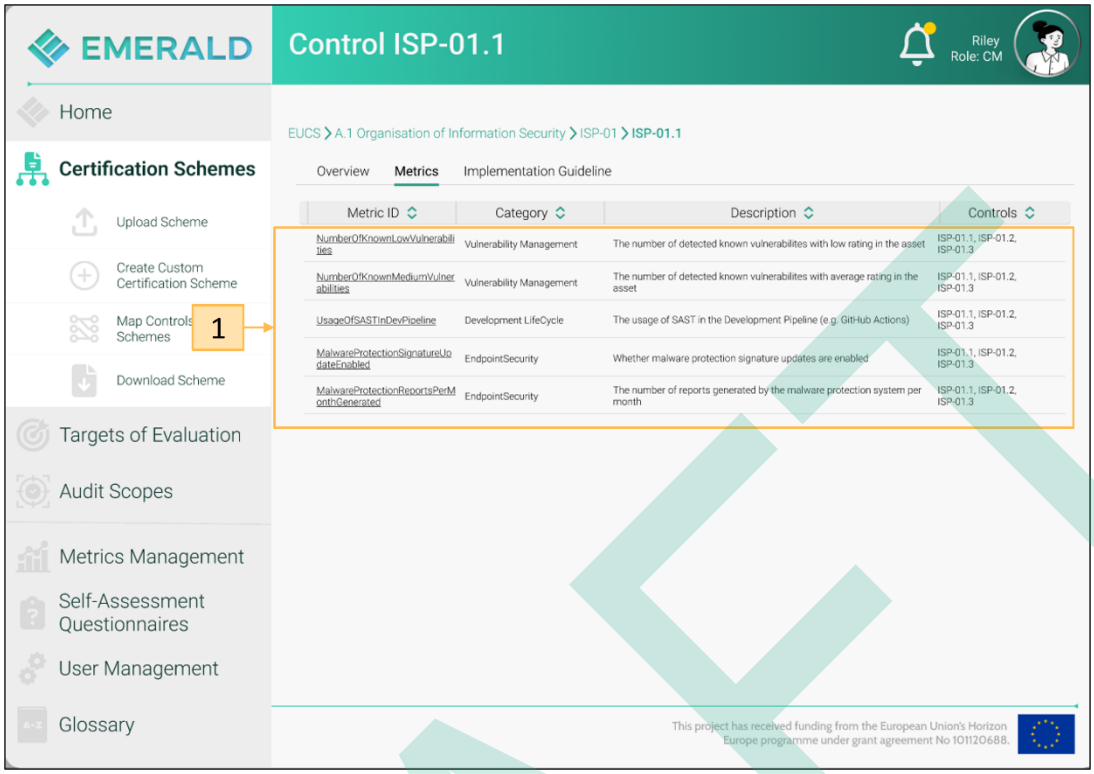

Figure 27. Certification Scheme – Browse Scheme – Metrics assigned

When clicking on the name of a control such as “NumberOfKnownLowVulnerabilities” detailed information of the metric is presented (see Figure 28).

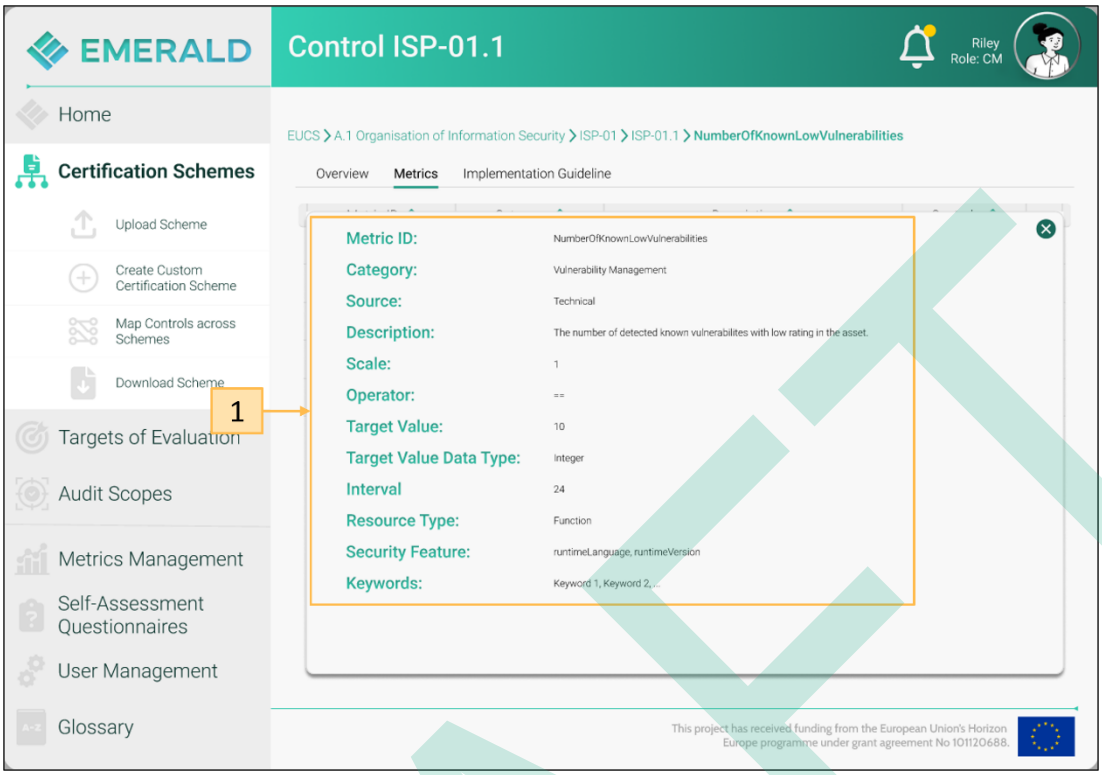

Figure 28. Certification Scheme – Browse Scheme – Metrics details

The last tab in Figure 29, point 1 (right) is the "Implementation Guideline" tab. If an implementation guideline was added to the control, it is shown as presented in Figure 29. The guideline provides some concrete suggestions and examples of how the corresponding control can be implemented.

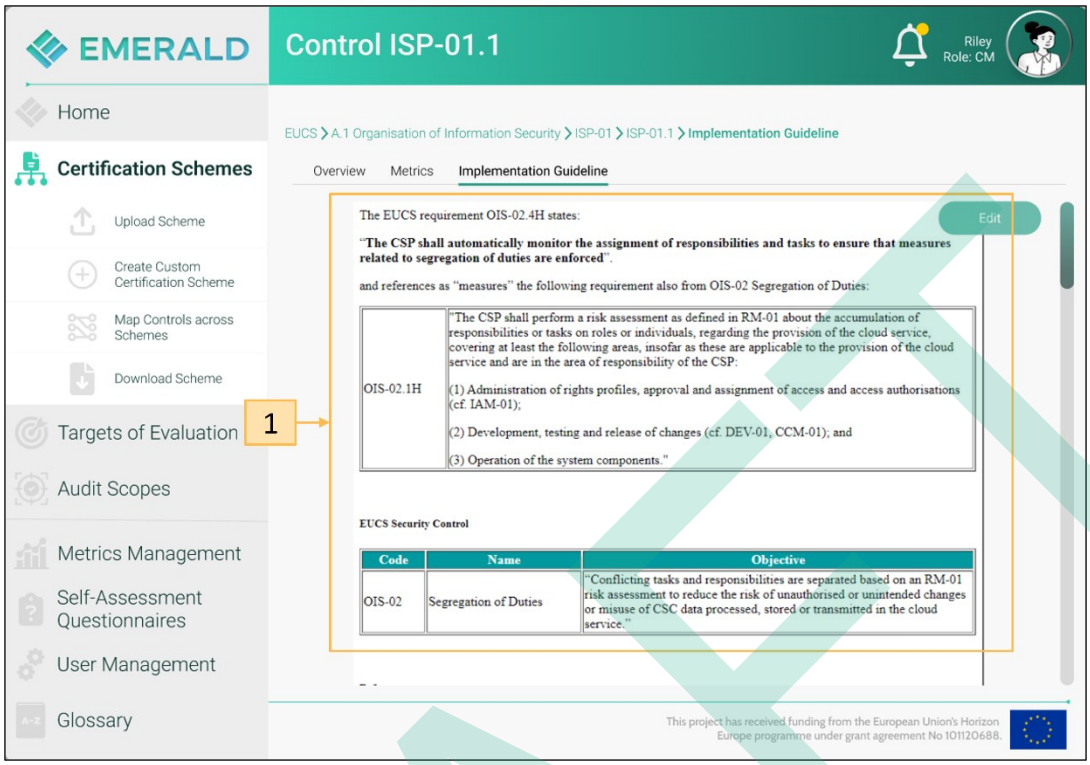

Figure 29. Certification Scheme – Browse Scheme – Control Implementation Guideline

To add an implementation guideline to a control, a user (depending on the user rights) needs to click on the implementation guideline upload button (see Figure 25, point 2). A pop-up window opens where the user can upload a prepared file via drag & drop – as presented in Figure 30, point 1.

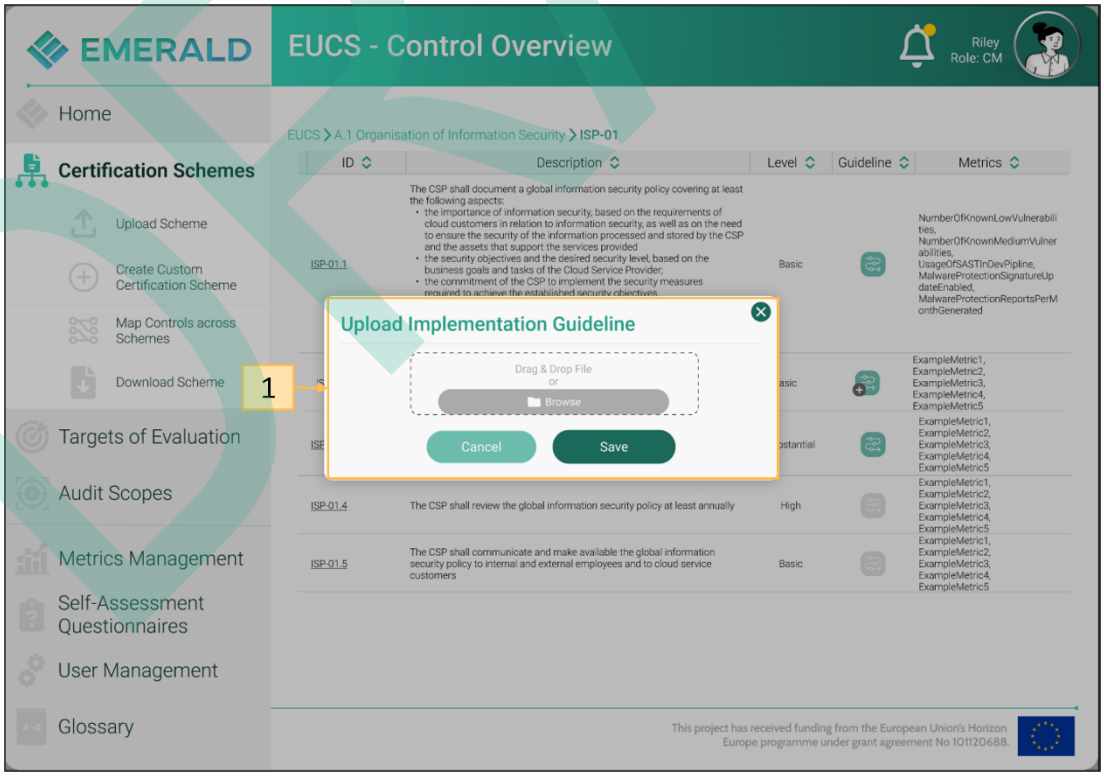

Figure 30. Certification Scheme – Browse Scheme – Upload Implementation Guideline

4.3.2 Mapping of metrics to controls

The mapping of metrics to controls is one core functionality of the EMERALD UI. To enter the mapping of metrics to control views, a user needs to click on Figure 23, point 6. Figure 31 presents the view, where a user is able to do the mapping of metrics to a control.

- **Manually Checked Controls**: Figure 31, point 1 presents the progress of how many controls and the suggested metrics have been manually checked by a user. By clicking on the progress bar, the user can filter for the checked or not checked controls.
- **Number of Metrics**: Figure 31, point 2 allows to adjust how many metrics should by suggested for a control by *MARI*.
- **Artificial Intelligence**: Figure 31, point 3 contains the AI Symbol. This symbol clearly states that AI is used in the background.
- **List of categories and controls**: Figure 31, point 4 offers the hierarchical structure of the controls, (sub-ordinate controls), and the individual controls.
- **Control and Status**: Figure 31, point 5 shows the currently active control “OIS01.1”. So far, this control is not marked with a green ok symbol (see Figure 31, point 6). This indicates that all metrics that have been automatically assigned to the control have not yet been manually checked by the user.
- **Metrics suggested**: Figure 31, point 7 shows the list with the metrics that have been suggested for the current controls. For each metric, the metric ID, the similarity score, a short description, its source, and the operator is shown. If a metric does not fit for the control it can be removed by unmarking the checkbox in front of the metric ID.
- **Add metrics**: If the list of metrics is missing a specific metric, the user can click on the “Add new” button (Figure 31, point 9), and below the list of all available metrics is opened (Figure 31, point 11). From this list the user can add other metrics that should be used for measuring the current control. After the user has adjusted the suggested control, the user clicks on the “Save” button (Figure 31, point 10). This save indicates at the same time that the current mapping of metrics to controls is approved.

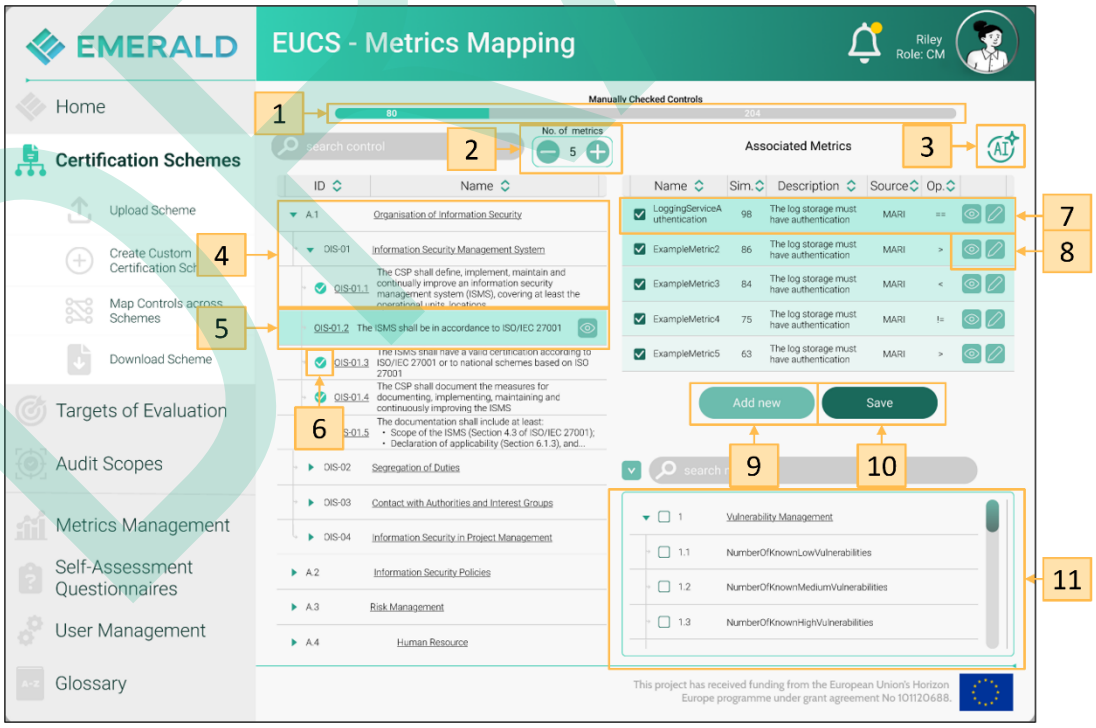

Figure 31. Certification Scheme – Mapping - Metrics to Controls

Besides adding a new metrics, it is also possible for a user to adjust the value of the metrics. Clicking on Figure 31, point 8 (left) a user gets more details about the metrics (not depicted). Clicking on Figure 31, point 8 (right) opens the edit view of a metric as shown in Figure 32 opens the metrics view in an edit mode as shown in Figure 32.

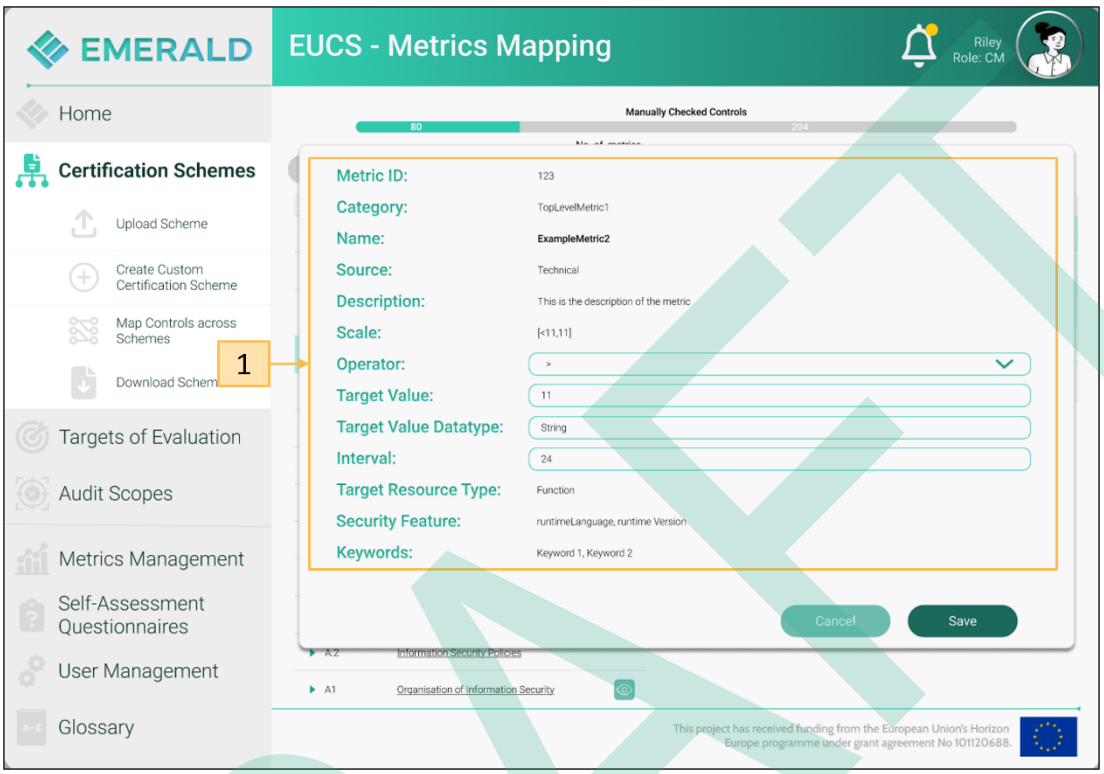

Figure 32. Certification Scheme – Mapping – Edit Metrics

4.3.3 Mapping of controls to controls across schemes

The mapping of controls to controls across schemes is another core functionality of the EMERALD UI. To enter the mapping of controls to control views, a user needs to click on Figure 23, point 4. Figure 33 presents the view, where a user is able to do the mapping of controls to controls across schemes. The functionality is similar to the mapping of metrics to controls (shown in Figure 31).

- **Scheme selection**: Figure 33, point 1 offers the user the possibility to select two schemes e.g. on the left side EUCS and on the right-side BSI C5, thus, the mapping is done from one control of EUCS to a control of BSI C5.
- **Artificial Intelligence**: Figure 33, point 2 shows the AI Symbol. This symbol clearly states that AI is used in the background.
- **List of categories and controls**: Figure 33, point 3 presents the hierarchical structure of the controls, (sub-ordinate controls), and the individual controls.
- **Control and Status**: Figure 33, point 4 shows the currently active control “OIS-01.2”. So far, this control is not marked with a green ok symbol (see Figure 33, point 5). This indicates that one or more controls of one scheme have been automatically assigned to the control of the other schema and that this mapping has not yet been manually checked by the user.
- **Control suggested**: Figure 33, point 6 shows that only one control of BSI C5 (OIS.01) is suggested to correspond to OIS-01.2 of EUCS. For each control, the control ID, the similarity score, a short description and its source is shown. If the suggested control of

BSI C5 does not match with the control of EUCS it can be removed by unmarking the checkbox in front of the control.

- **Add control**: If the list of suggested controls (right) does not fit to the control (left side), the user can click on the "Add new" button (Figure 33, point 7), and below the list of all available controls of BSI C5 is opened (Figure 33, point 9). From this list the user can add another control that corresponds to the control of EUCS. After the user has adjusted the suggested control, the user clicks on the "Save" button (Figure 33, point 8). This save indicates at the same time that the current mapping of controls to controls is approved.

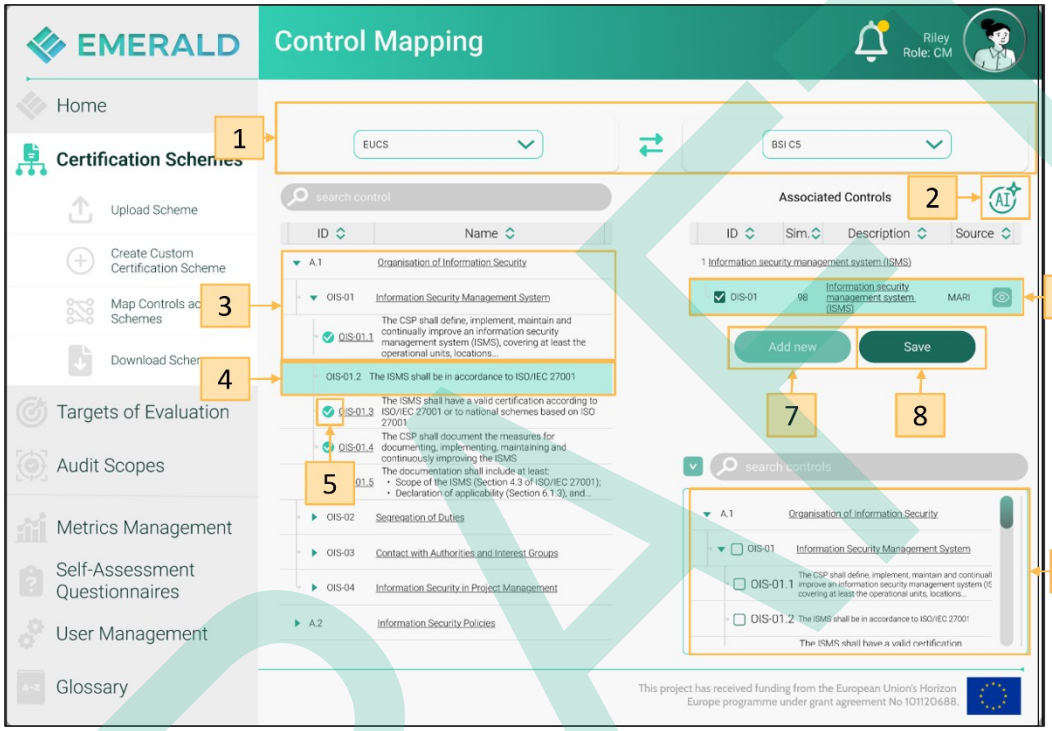

Figure 33. Certification Scheme – Mapping - Controls to Controls

When clicking on the "Save" button, the user has also the possibility to take over the metrics that have been assigned to the control of the left side (the control of EUCS) to the control of the right (in the example to BSI C5) as shown in Figure 34. When clicking on the checkbox (see in Figure 34, point 1), the user can choose to take over the metrics. Figure 34, point 2 shows which metrics are available and will be taken over. Still a user has the possibility to select which metrics should be taken over.

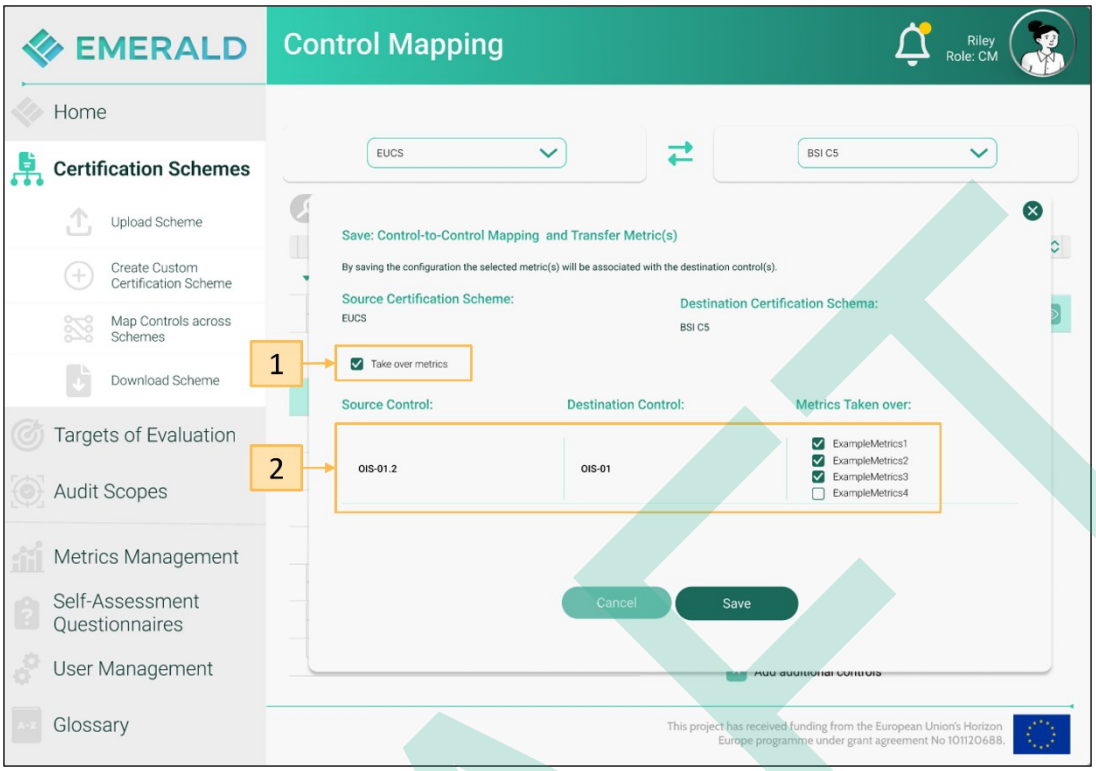

Figure 34. Certification Scheme – Mapping - Take over Metrics

4.3.4 Create your own certification scheme

In EMERALD it is also possible to create your own certification scheme. Clicking on Figure 23, point 3 opens the following view as shown in Figure 35. To create a new scheme, a user needs to add a name (Figure 35, point 1), a description for the scheme (Figure 35, point 2), and a version (Figure 35, point 3). Clicking on the "Next" button (Figure 35, point 4) guides the user to the page (see Figure 36) where categories and/or controls from existing schemes can be selected and added to the new scheme.

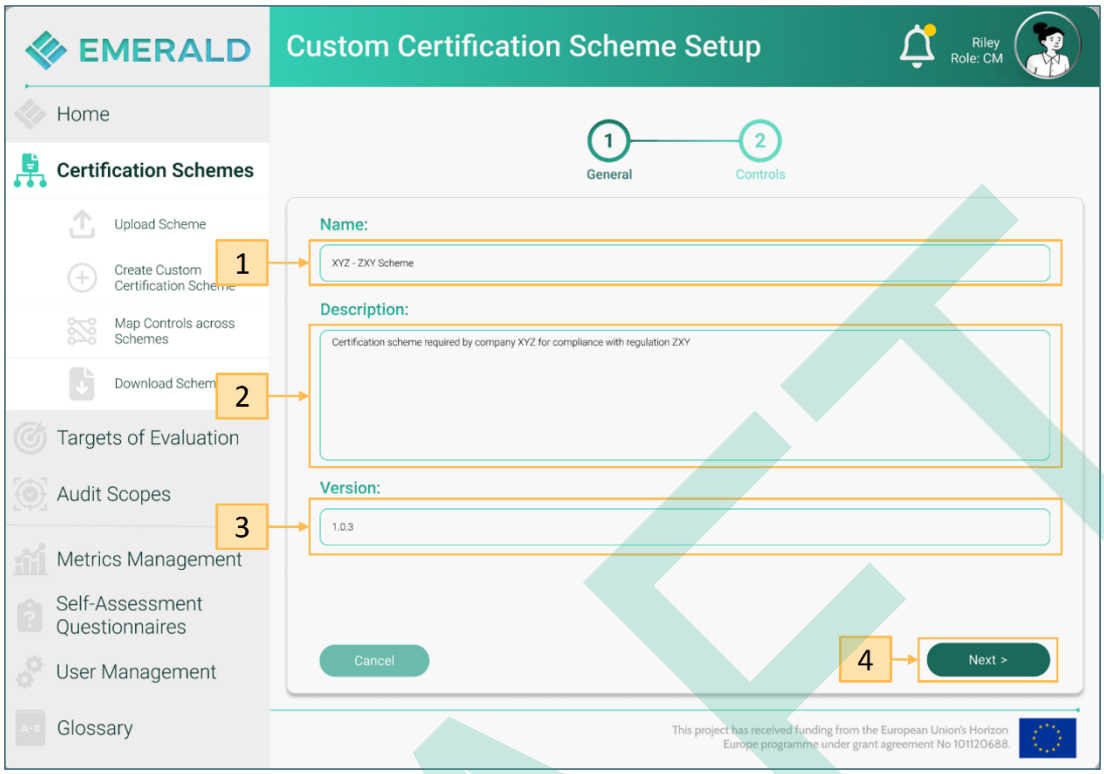

Figure 35. Certification Scheme – Create New Certification Scheme - Overview

Figure 36, point 1 provides a list with all available certification schemes. All schemes are browsable, and a user can either select whole categories or individual controls to be added to the newly created scheme. For example, in Figure 36 the user has selected one control "OIS-02" of BSI-C5 and the whole category "A2" from EUCS for the new scheme (see Figure 36, point 2).

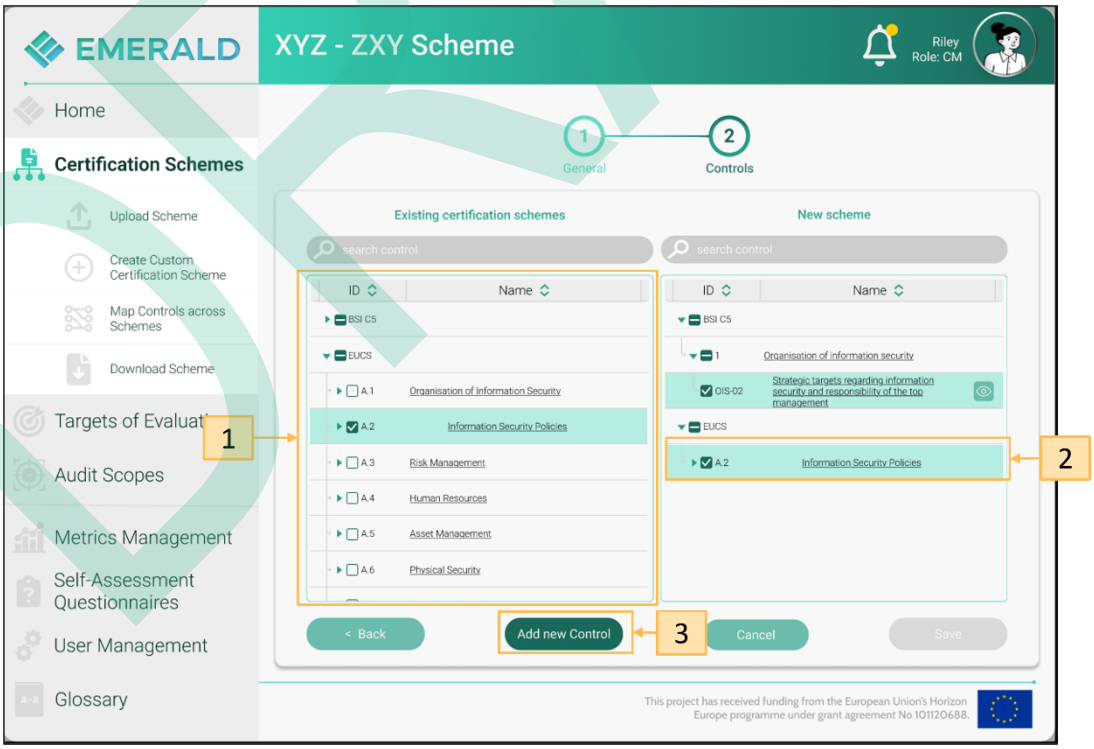

Figure 36. Certification Scheme – Create New Certification Scheme - Select Categories and Controls

When clicking on the "Add new Control" button (see Figure 36, point 3) a user has the possibility to add a newly created control. To create a new control, a user has to enter a unique ID (Figure 37, point 1), has to enter a name for the control (Figure 37, point 2), has to select a category (Figure 37, point 3), and add a description of the control (Figure 37, point 4). When scrolling down, the user can add information if the newly created control is related to a control of an existing schema (see Figure 38, point 1). And additionally, the user can select one or more metrics for the control schema (see Figure 38, point 2). This control will then be added to the newly created scheme as presented in Figure 39, point 1.

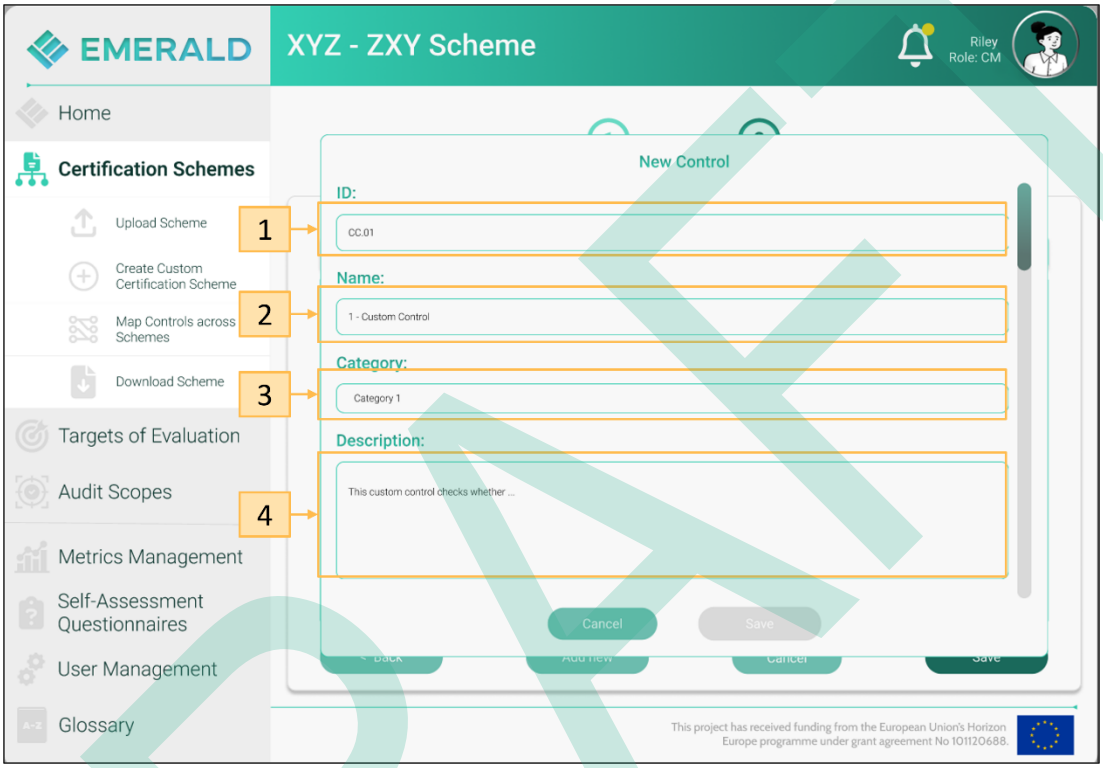

Figure 37. Certification Scheme – Create New Certification Scheme - Create new Control 1

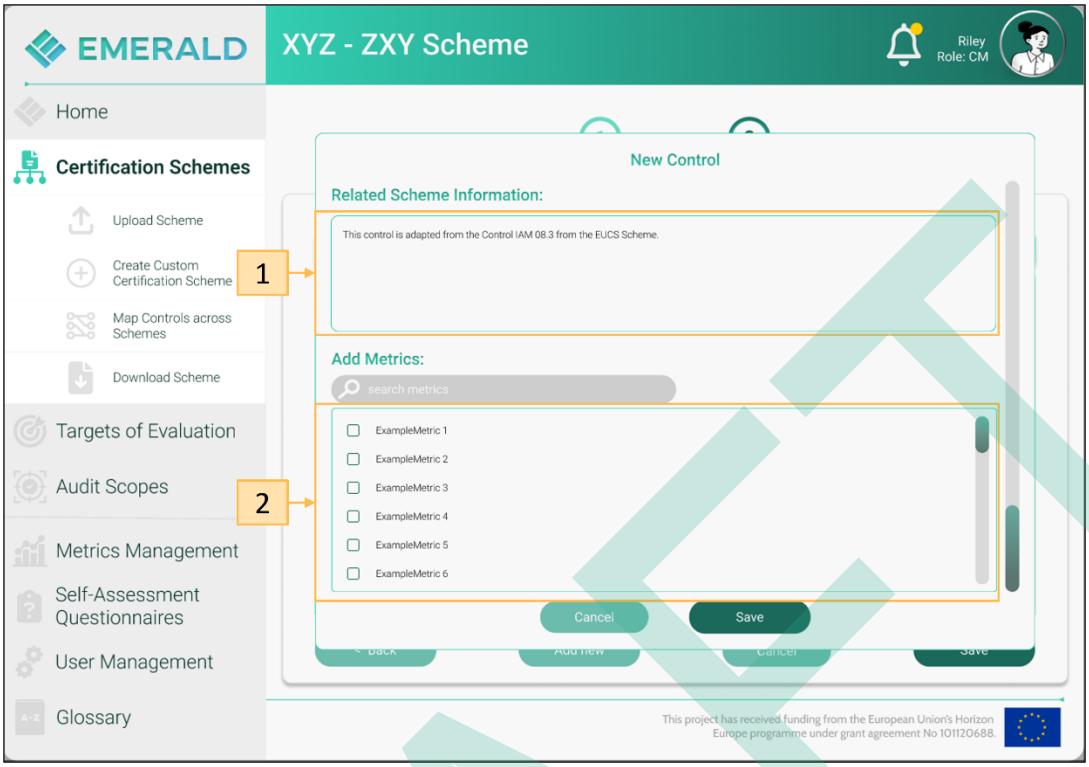

Figure 38. Certification Scheme – Create New Certification Scheme - Create new Control 2

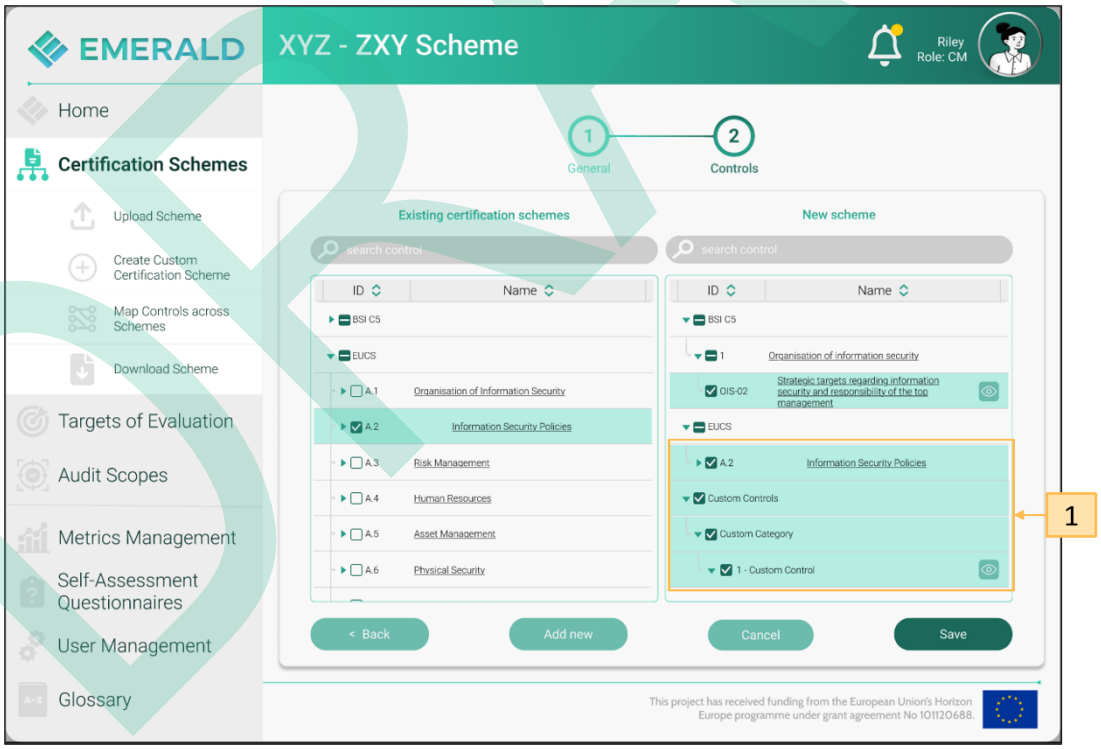

Figure 39. Certification Scheme – Create New Certification Scheme - New Control added

4.3.5 Upload and download certification schemes

To upload a certification scheme that is available in OSCAL[5] or as an MS Excel file, a user needs to click on Figure 23, point 2. For the scheme, the user needs to enter a name (see Figure 40, point 1), a description (see Figure 40, point 2), and a version number (see Figure 40, point 3). Then the user can upload the file via Drag & Drop (see Figure 40, point 4). When clicking on the "Save" button (see Figure 40, point 5), the newly uploaded scheme will be made available in the scheme overview page (Figure 21).

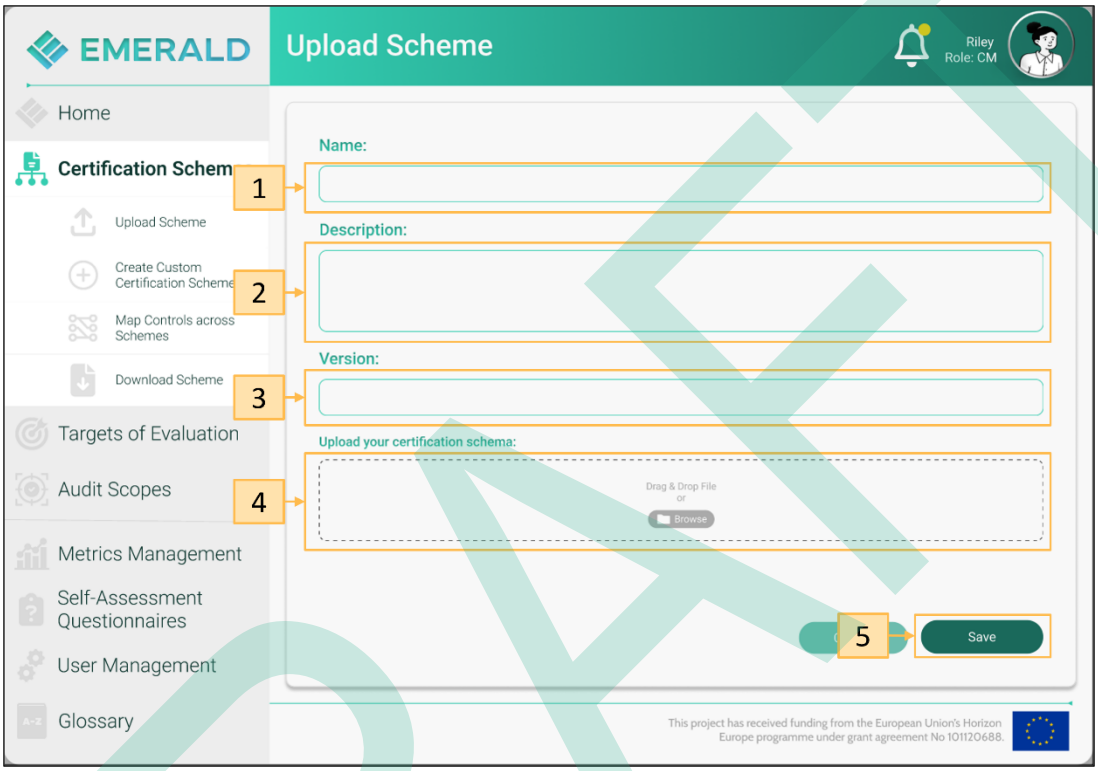

Figure 40. Certification Scheme – Upload Scheme

Figure 21, point 5 offers the possibility to download an existing scheme. As shown in Figure 41, the user needs to select the respective scheme (see, point 1), decide in which format the download file should be (see Figure 41, point 2), and click on the "Download" button (see Figure 41, point 3) to download it.

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

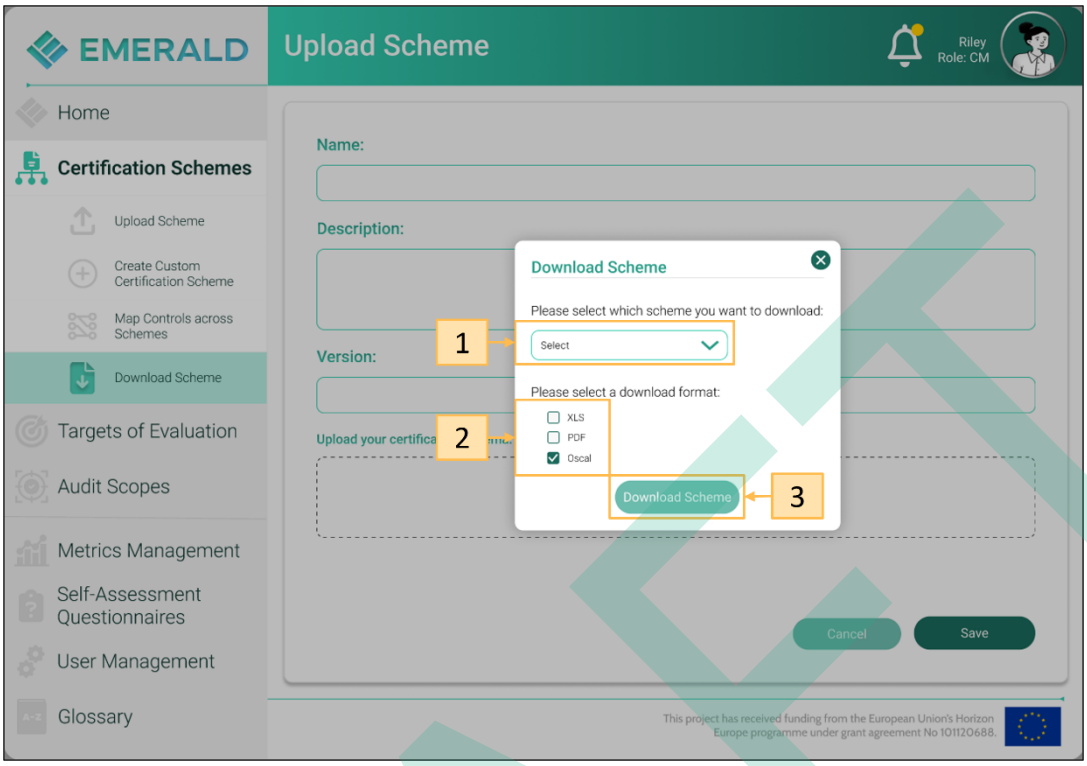

Figure 41. Certification Scheme – Download Scheme

4.4 Setup and Manage Targets of Evaluation

Stream 2: Setting up and managing the targets of evaluation focuses on the creation of targets for certification (e.g., cloud services, ...). During the setup phase, the UI offers the installation guidelines for installing different evidence extractors (Evidence extractors need to be set up on the respective environment of the target of evaluation, and the installation cannot be done via the EMERALD UI). It allows users to enable or disable the *TWS* as needed and to manage access rights for the corresponding target of evaluation.

After initially setting up a target of evaluation, the user can manage it within EMERALD. This includes updating general information (such as name, *TWS*, and user assignment), managing evidence extractors (e.g., downloading installation guidelines, updating statuses, and providing data for the *AI-SEC*), uploading policy documents, reviewing resources and evidence, and managing certifications.

Figure 42 presents an overview of what a user is able to do in the target of evaluation visualisation stream.

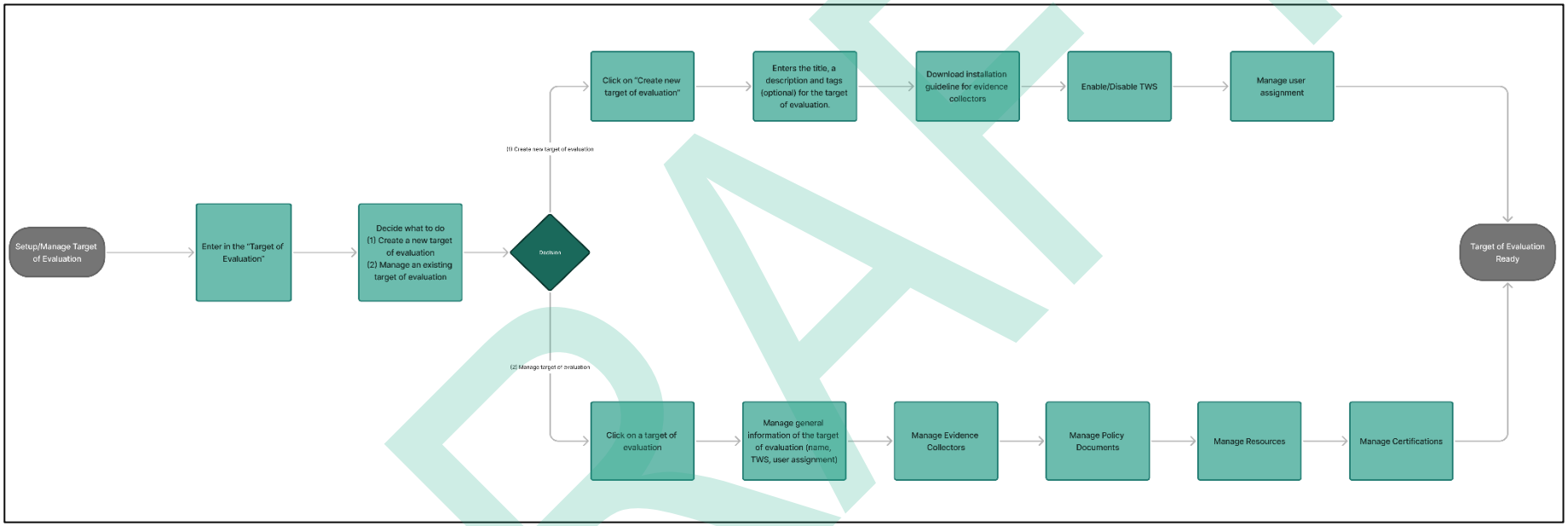

Figure 42. Setup and Management of the Target of Evaluation Process in the EMERALD UI

When entering target of evaluation section in the EMERALD UI, a list of targets of evaluation is presented (in-line with the access rights of the user) as shown in Figure 43. Figure 43, point 2 presents the targets of evaluation the current user is allowed to see. For each ToE, the resource status is presented: green means all assessment result retrieved from the resources are ok, while read means, some assessment results are not ok, and a user has to have a closer look at it. Then the list presents the type of the cloud service (e.g. cloud) and a short description of the ToE. Finally, the current user (depending on the access rights) has also the possibility to delete an existing ToE.

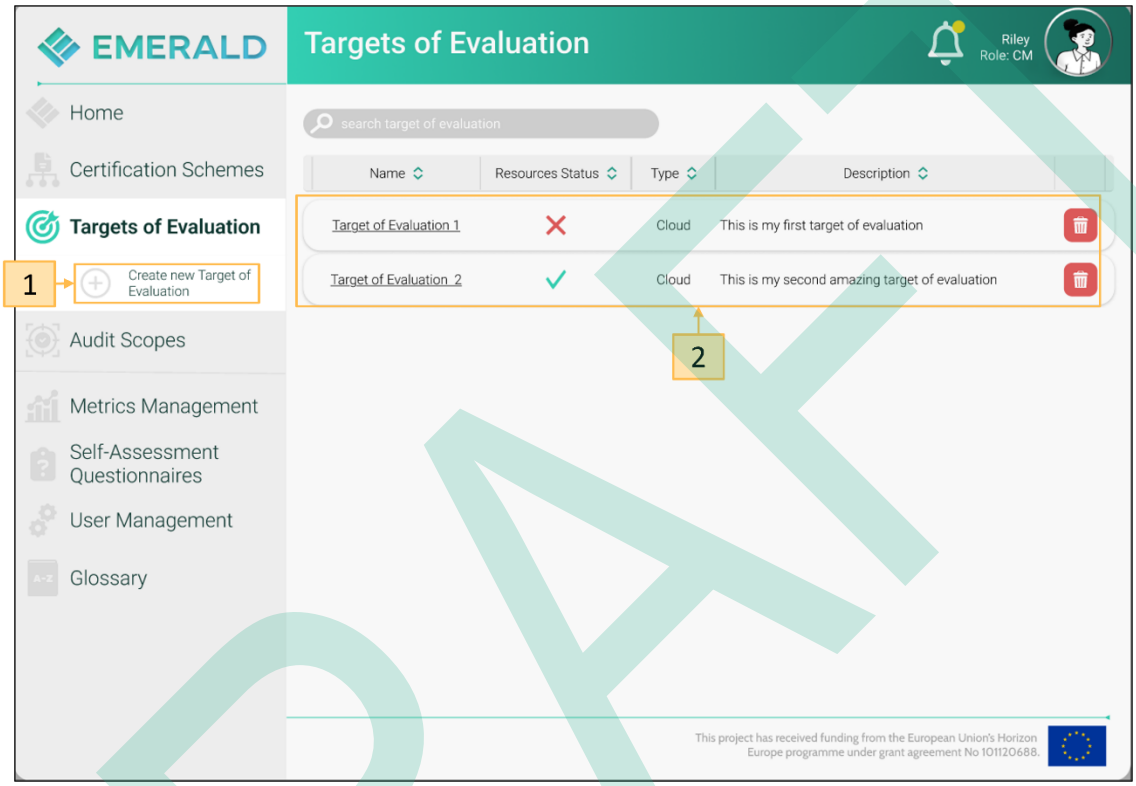

Figure 43. Target of Evaluation – Overview

4.4.1 Setup Targets of Evaluation

When clicking on the “Create new Target of Evaluation” on the left (see Figure 43, point 1), the current user can create a new target of evaluation. Figure 44 presents the first step of setting up a new target of evaluation. Figure 44, point 1 presents the four steps that need to be fulfilled to set up a new target of evaluation. In the first step, a user enters a name (Figure 44, point 2) and a short description (Figure 44, point 3), adds some tags (Figure 44, point 4) and selects the type of the ToE (Figure 44, point 5). After clicking “Save”, the ToE gets assigned a unique target id (not depicted in Figure 44).

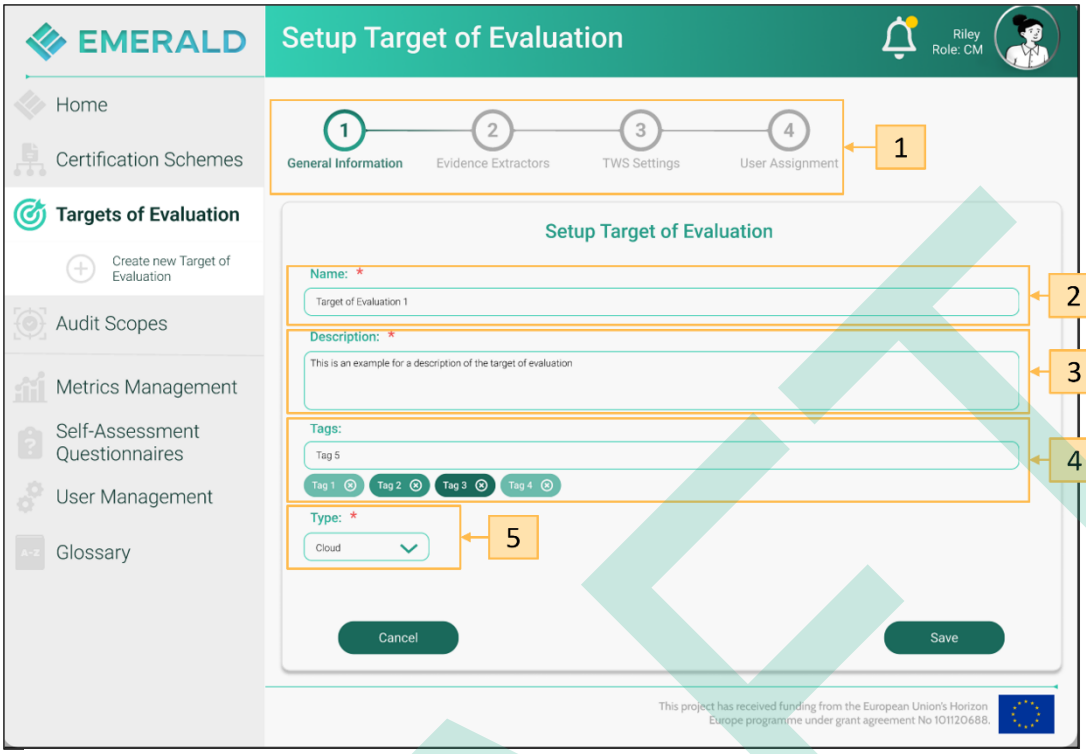

Figure 44. Setup a Target of Evaluation – General Information

In the next step presented in Figure 45, a user gets all the necessary information on how to install the relevant evidence extractors for the ToE. Figure 45, point 1 just shows the available evidence extractors, and when clicking on Figure 45, point 2, a pop-up window is opened as shown in Figure 46.

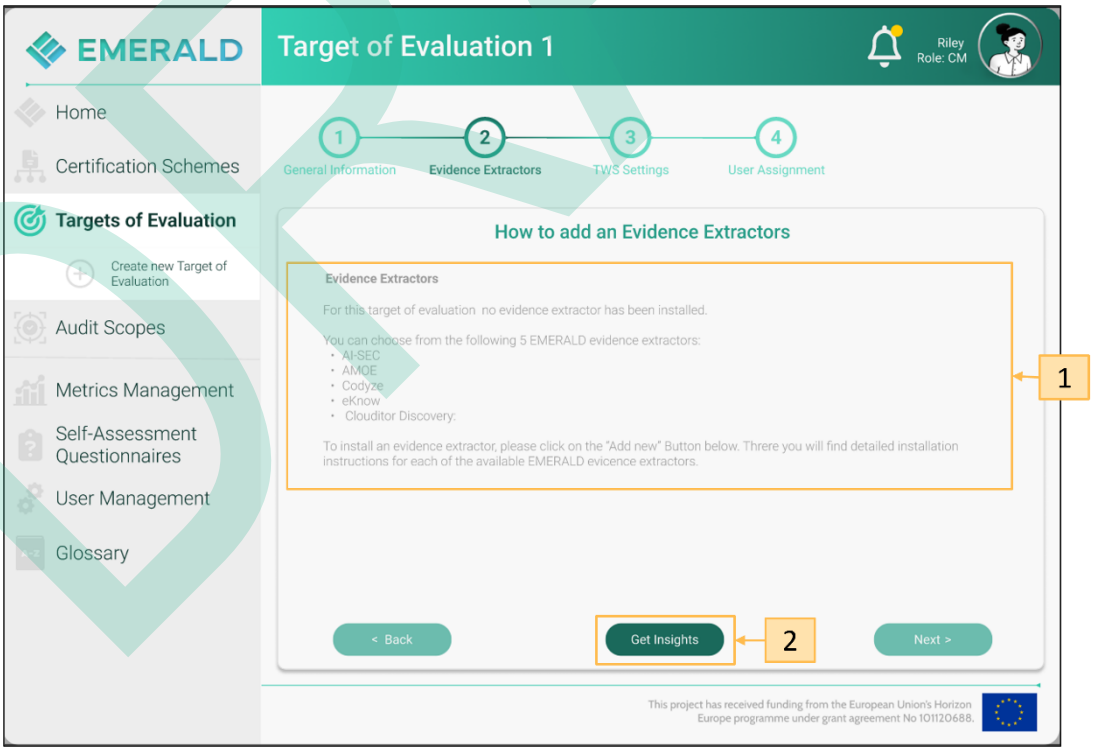

Figure 45. Setup of ToE – Step 2 – List of Evidence Extractors

Figure 46 provides for each evidence extractor a detailed description on how to install it – this information can also be downloaded. It consists of an installation guideline and some source code that needs to be adapted so that the extractor is connected to the ToE. For example, the description presents the Target ID of the current ToE and the Evidence Extractor URL offered by the *Orchestrator* (see Figure 46).

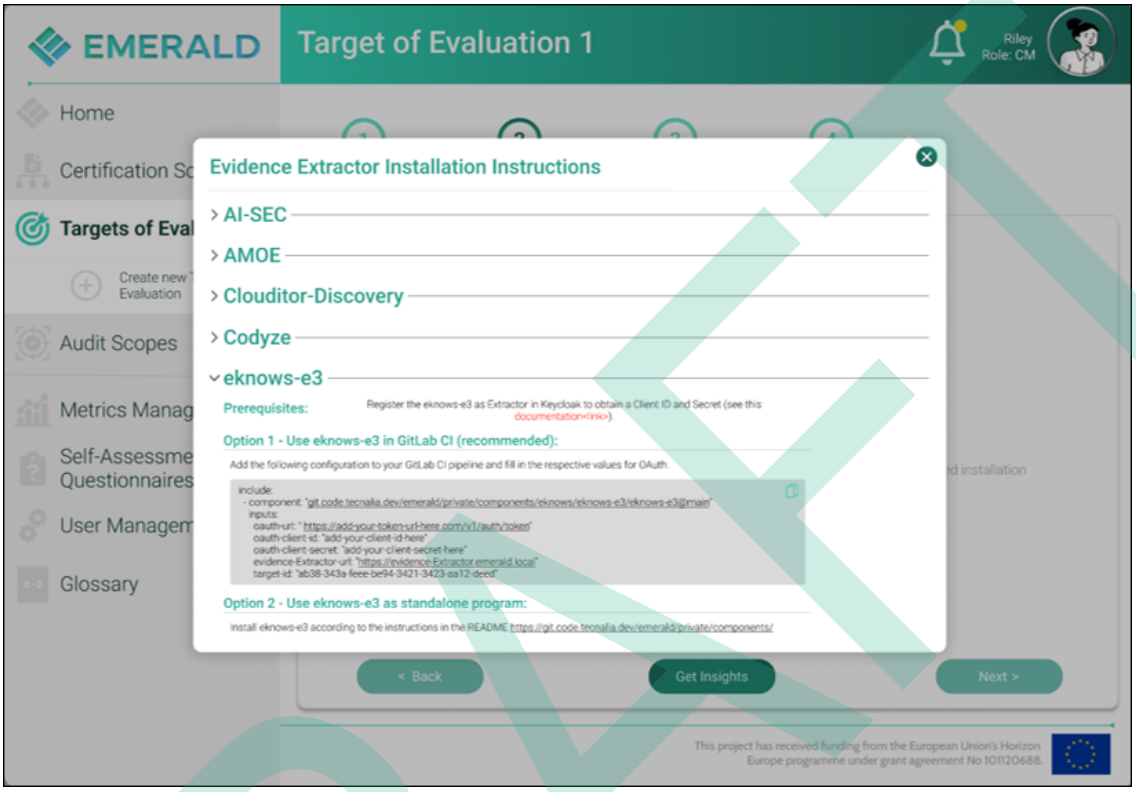

Figure 46. Setup of ToE – Step 2 – Evidence Extractor Installation

In the third step of the ToE setup, settings regarding the *Trustworthiness System* (*TWS*) can be adjusted. Here, a user can define when and how often the integrity validation is performed in the *TWS* - automatically and/or on demand, as depicted in Figure 47. Options are:

- Always, when entering a respective audit scope
- On demand by the user
- Automatically every 1, 5, 10, or 15 minute(s).

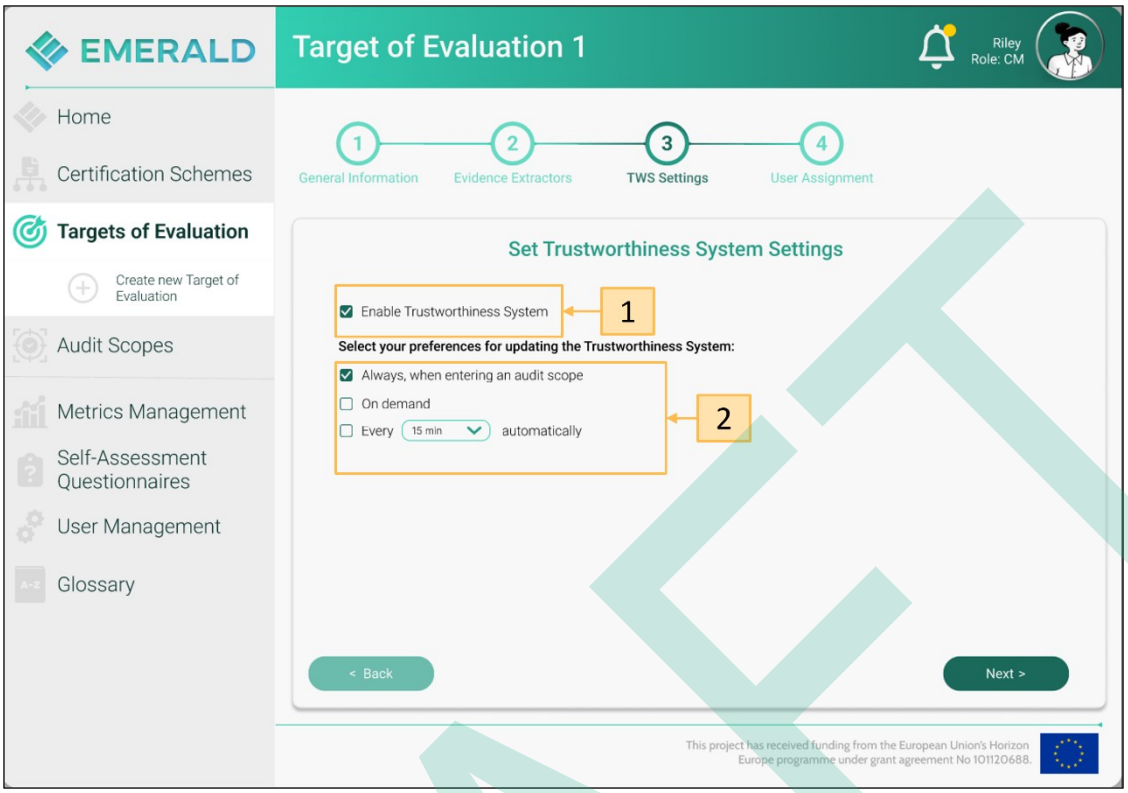

Figure 47. Setup of ToE – Step 3 – TWS Settings

The fourth step allows to deal with the user assignment as presented in Figure 48. Figure 48, point 1 allows to search for a user. Below is a list of all users in the EMERALD instance. For each user, one sees if the user has access to the current ToE, the name of the user, and the role (Figure 48, point 2). When clicking on "Save" (Figure 48, point 3), the new ToE is created.

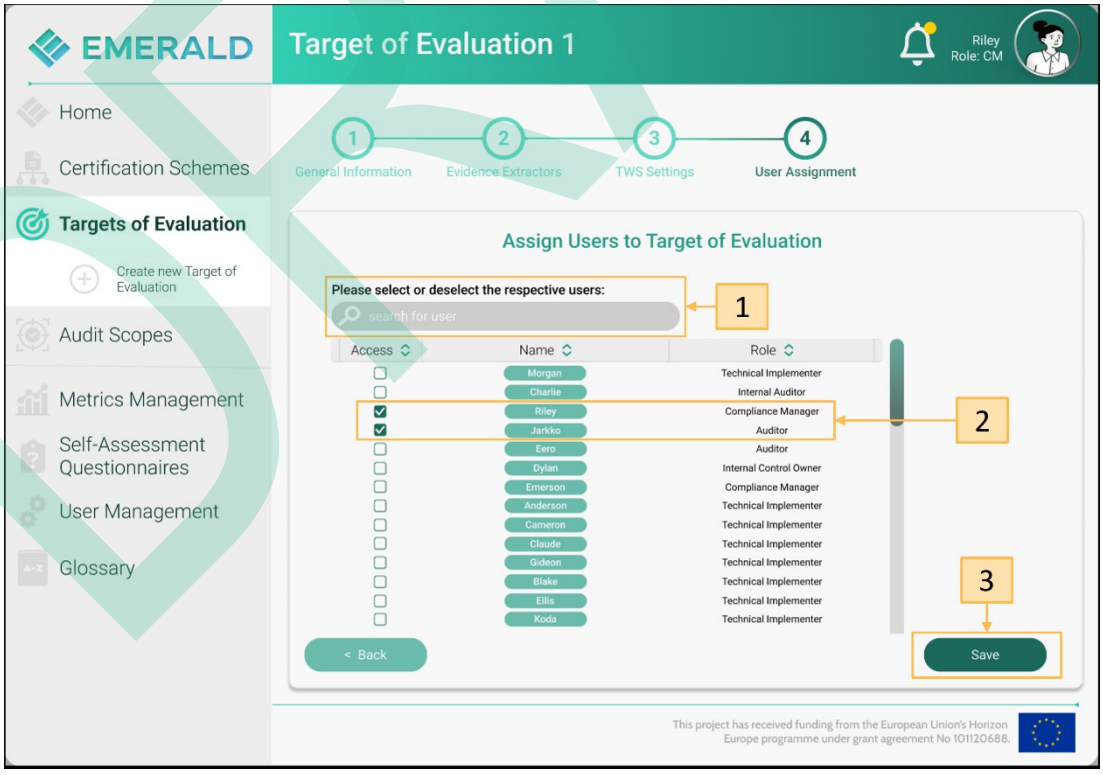

Figure 48. Setup of ToE – Step 4 – User Assignment

4.4.2 Manage Targets of Evaluation

After having created a new ToE, a user has the possibility to manage the newly created ToE. Therefore, the user needs to click on the Targets of Evaluation (see Figure 21, point 3) and then click on the name of the ToE like “Target of Evaluation 1” in the overview page (see Figure 43).

When entering a ToE, the following view is presented as shown in Figure 49. Using the tabs in Figure 49, point 1 allows a user to go through all the pages, that offer the management of the ToE. These include beside the “Information View”, the evidence extractors, the policy documents, the resources and the certifications.

Figure 49 shows the “Information View”. Figure 49, point 2, presents the general information about the ToE. Figure 49, point 3, shows if the TWS is enabled or disabled and which settings were selected. Figure 49, point 4, shows the status of the user assignment.

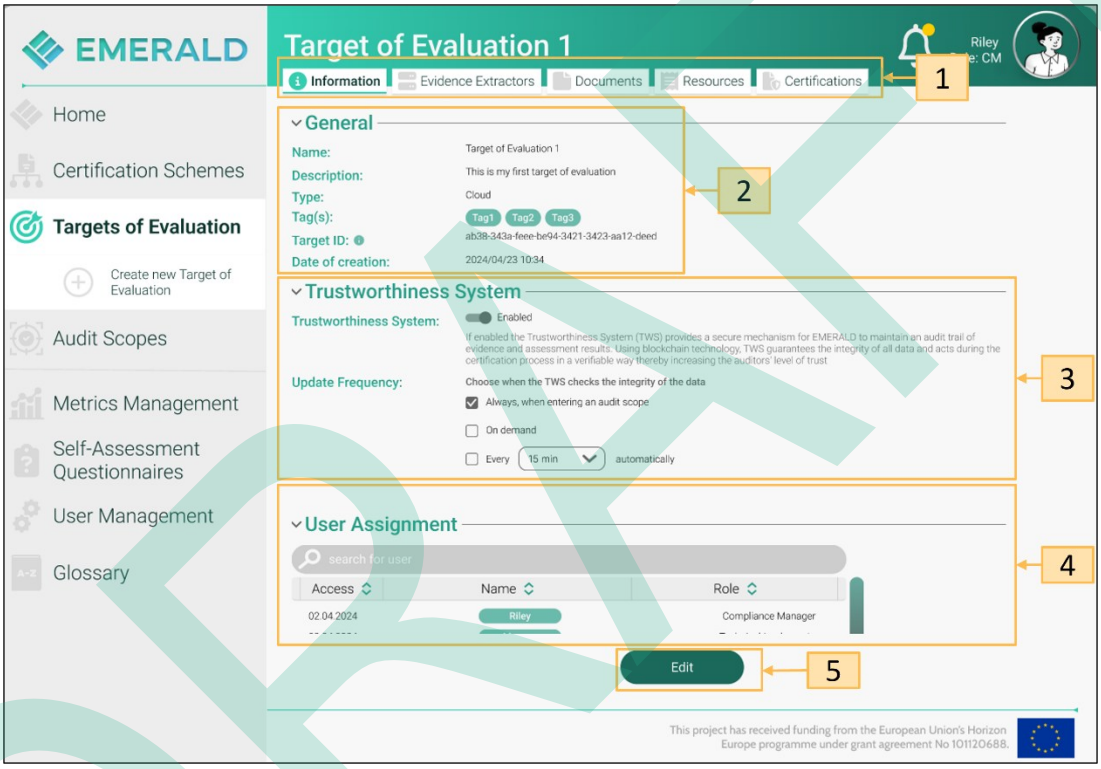

Figure 49. Manage ToE – Information

When clicking on the “Edit” button (Figure 49, point 5), the same page is shown in edit mode, thus, a user can change the following parts as presented in Figure 50. In Figure 50, point 1, the name, the description, and the ToE type can be changed. In Figure 50, point 2, the TWS can be enabled and disabled, and the settings can be changed. In Figure 50, point 3, the user assignment can be changed. When clicking on the “Save” button (Figure 50, point 4) all changes are stored.

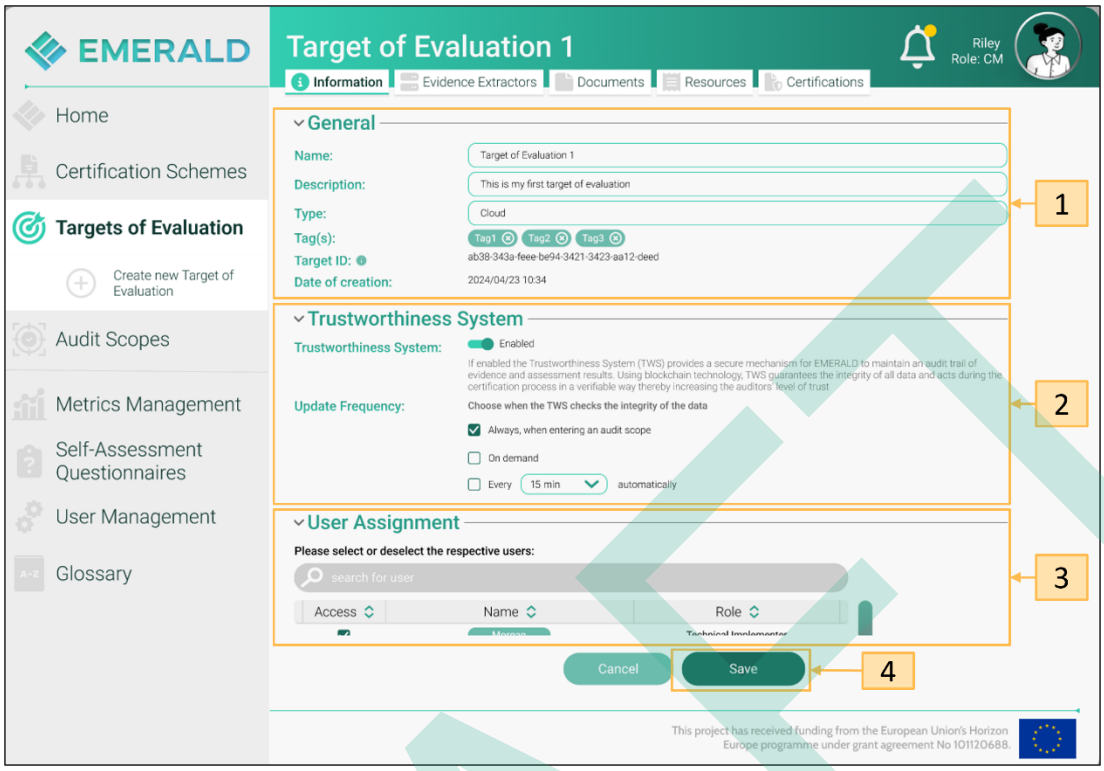

Figure 50. Manage ToE – Edit Information

When clicking on the tab “Evidence Extractors” (see Figure 51, point 1), all installed evidence extractors for the ToE are shown, as presented in Figure 51. For each extractor, one sees the status of it (active or paused), the extractor’s name, and when the last evidence was extracted (see Figure 51, point 2). When clicking on Figure 51, point 3, the user gets the description of how to install other available extractors as already shown in Figure 46.

After installing the evidence extractors *AMOE* and *AI-SEC*, additional functionality is available in the EMERALD UI.

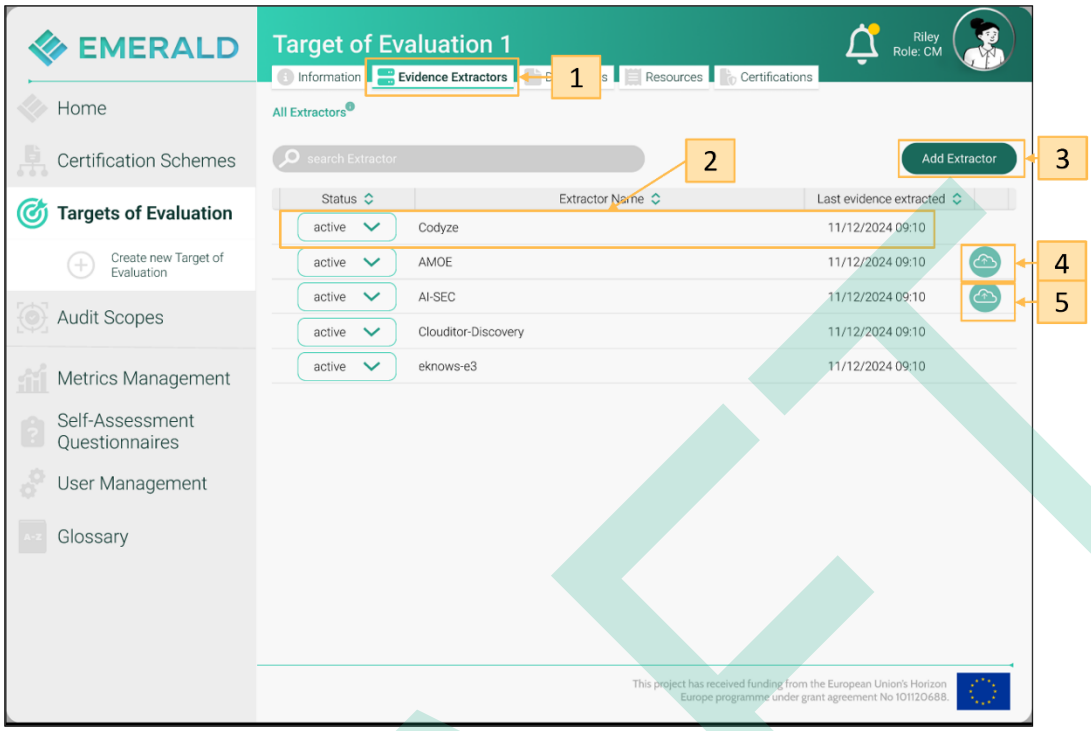

Figure 51. Manage ToE – Evidence Extractors

When clicking on Figure 51, point 5, a view opens that allows to upload models or data information that is used by *AI-SEC* (see Figure 52). Documents needed for *AI-SEC* are model information and data information. Models can be uploaded either using an URL or by uploading a file (see Figure 52, point 1). Data for the model can be uploaded via files (see Figure 52, point 2). All uploaded documents are presented in a list as shown in Figure 52, point 3.

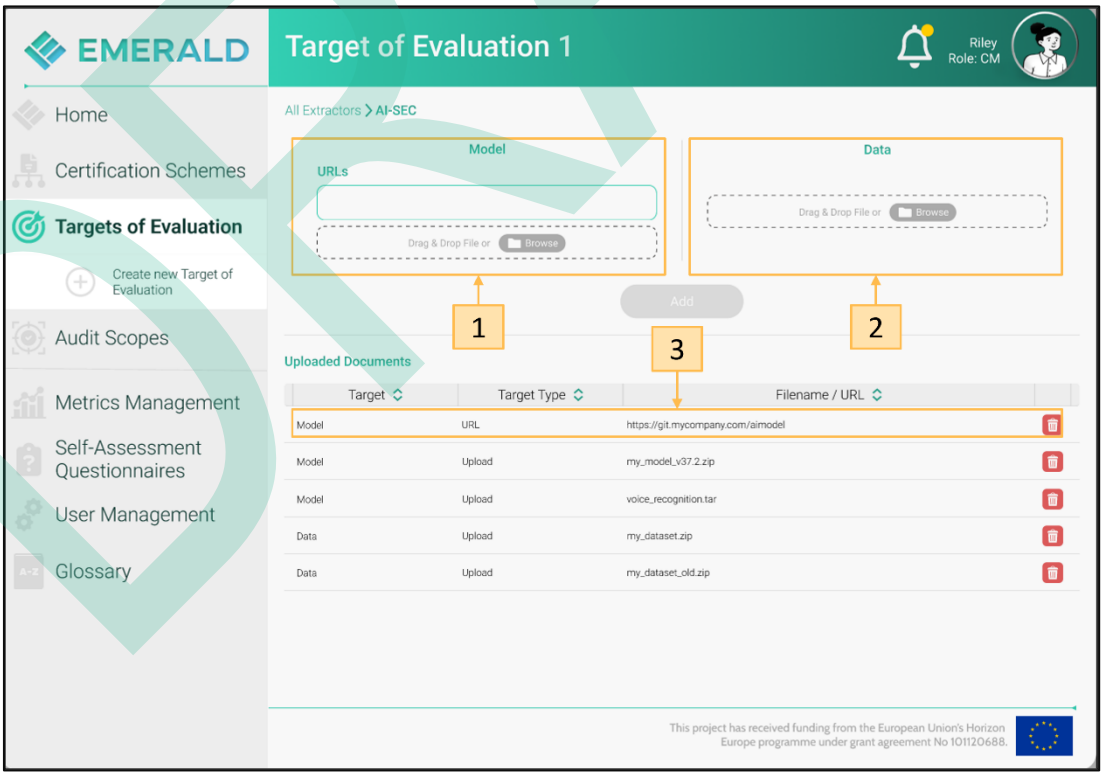

Figure 52. Manage ToE – AI-SEC Information

When clicking on Figure 51, point 4, a user is guided to the "Documents" tab (to be used by *AMOE* extractor), as presented in Figure 53. This view presents a list of all uploaded policy documents (Figure 53, point 1). For each document, it shows the decision status of the assessment results, the associated metrics, by whom the document was uploaded, and the upload date.

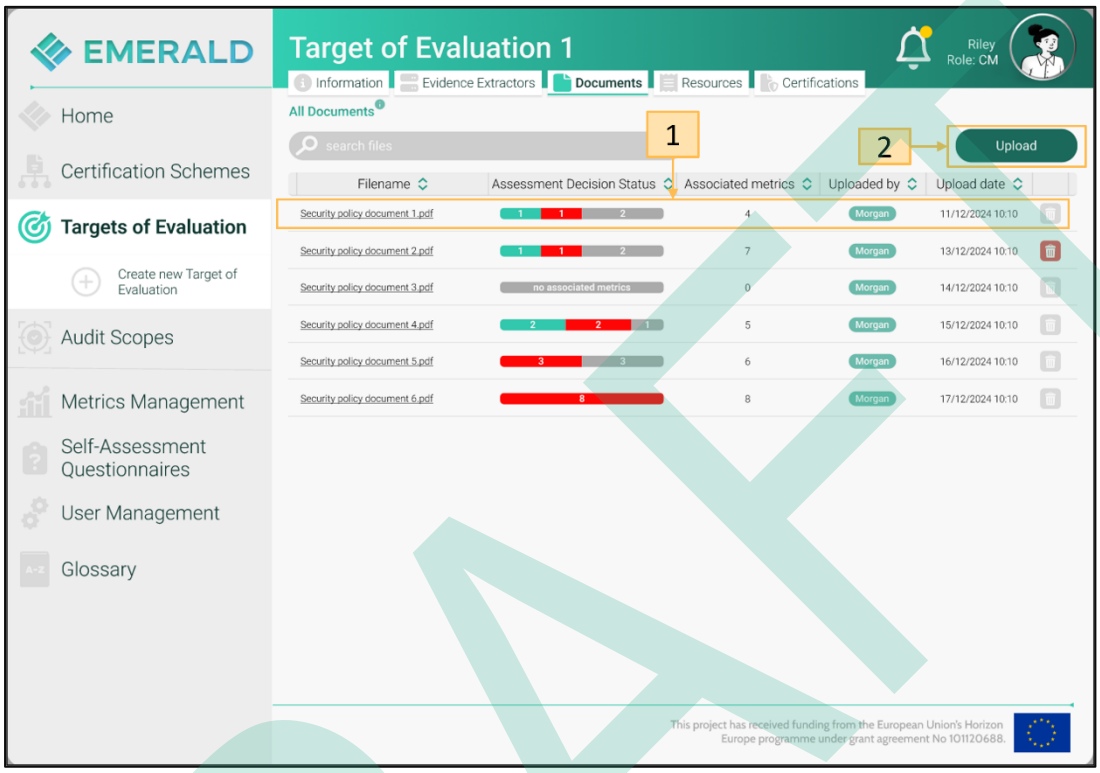

Figure 53. Manage ToE – AMOE Documents

When clicking on the "Upload" button (Figure 53, point 2), a new policy document can be uploaded (see Figure 54). With drag & drop, a user can drag a new policy document to the view to be uploaded (see Figure 54, point 1). Second, the user needs to define which metrics should be extracted from the policy document (see Figure 54, point 2). When clicking on "Save" (see Figure 54, point 3), the document will be uploaded and stored, and the respective assessment results for the metrics will be extracted.

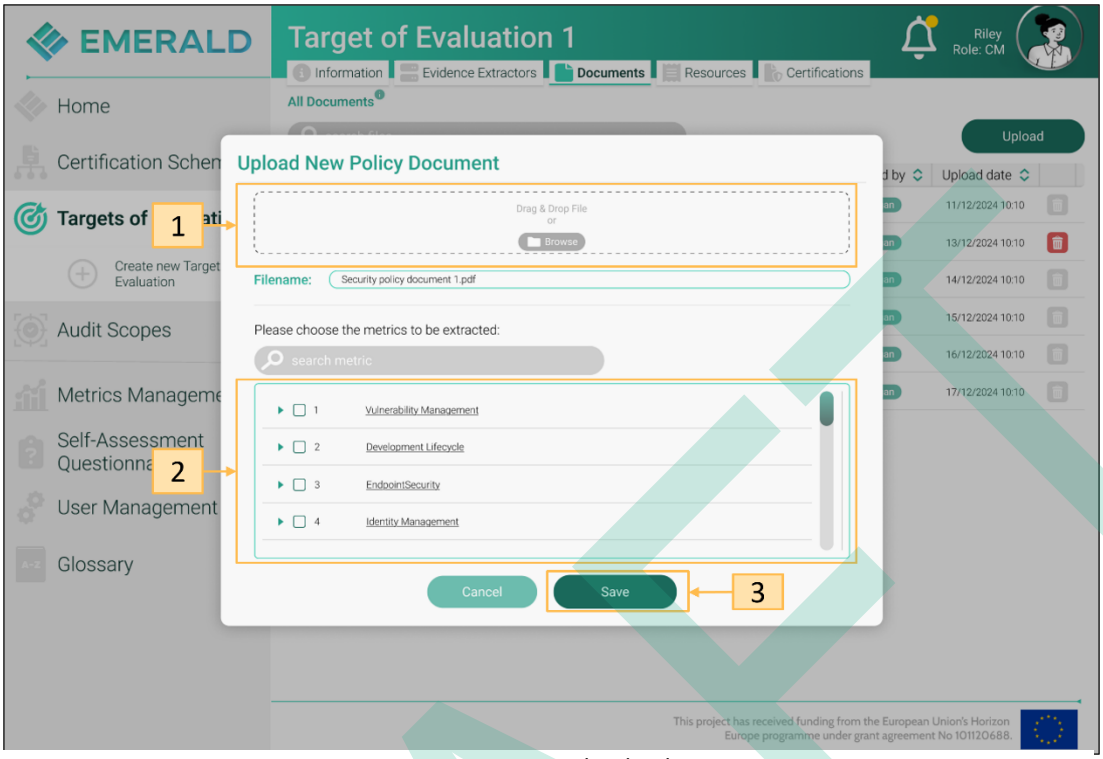

Figure 54. Manage ToE – Upload Policy Document

After uploading a policy document, the user can access more detailed information regarding the policy document. The evidence view shows information about the extracted evidence (Figure *55*). By clicking on "information" (Figure *55*, point 4) the user can open the information view to get more insights about the just uploaded document (Figure 56).

In the evidence view, each evidence is shown in a row with the assessment decision, evidence ID, status, metric ID, and extraction date (Figure *55*, point 1). When all evidence has been checked manually by the user (Figure 57), it can be committed to the *Evidence Store* (Figure *55*, point 2). The user also has the possibility to add an additional metric to be extracted from the policy document (Figure *55*, point 3). And the user is also able to search for evidence (Figure *55*, point 5).

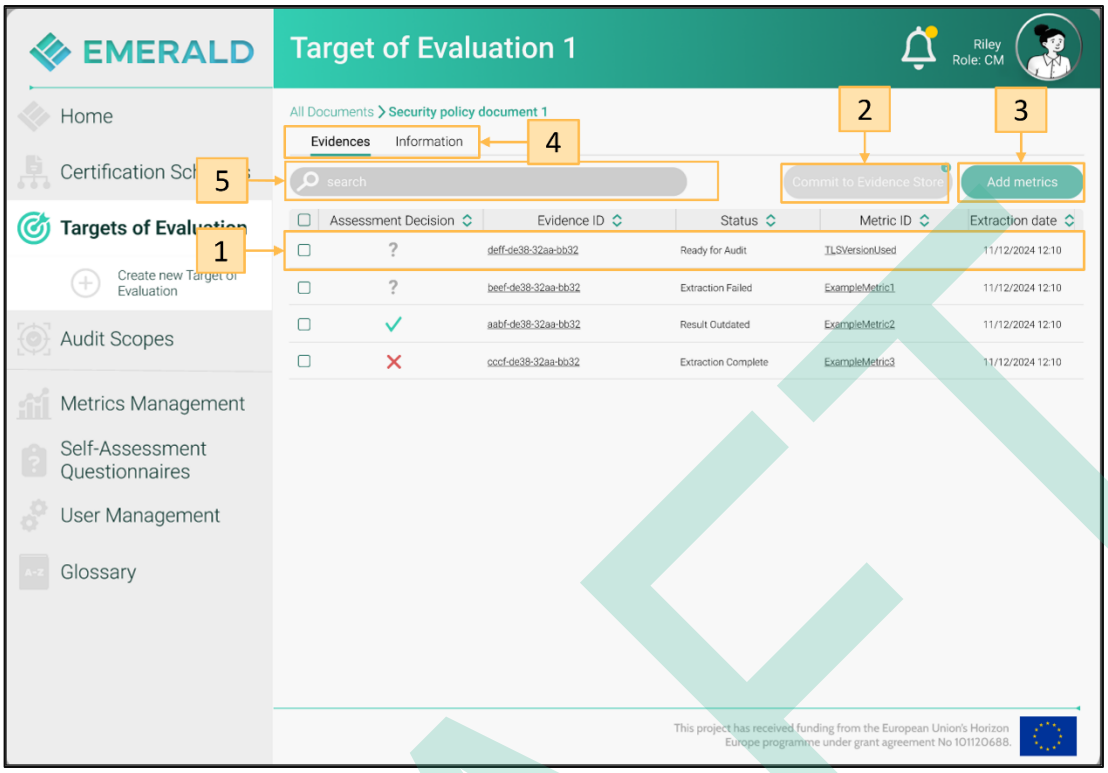

Figure 55. Manage ToE – Security Policy Document Evidence View

More detailed information about the policy document is depicted in Figure 56. The user can see details such as the filename, file ID, uploaded by, upload date, status (Figure 56, point 1). Additionally, the user can also download (Figure 56, point 2) the policy document or delete the policy documents (Figure 56, point 3).

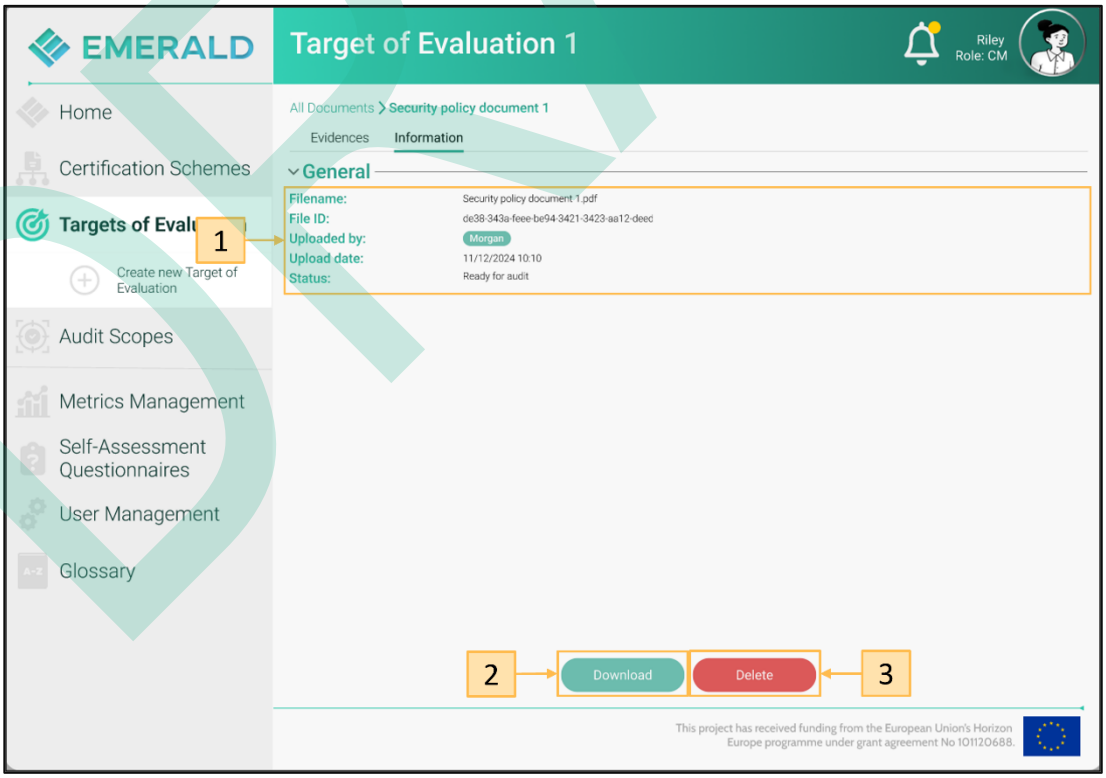

Figure 56. Manage ToE – Security Policy Document Information View

For each evidence the user needs to review the automatic assessment hints (Figure 57). The user can review the general file, metric and assessment information (Figure 57, point 1). Additionally, the user is also able to review the information as an html (Figure 57, point 2) or pdf file (Figure 57, point 3). Based on the extracted information the user needs to decide if the evidence provided proofs the metric and is complaint via selecting either “compliant” or “non-compliant” and providing an assessment comment (Figure 57, point 4). In EMERALD all content that has been generated with the support of AI is marked with an AI Icon (Figure 57, point 5). The added information of the user is automatically saved by EMERALD.

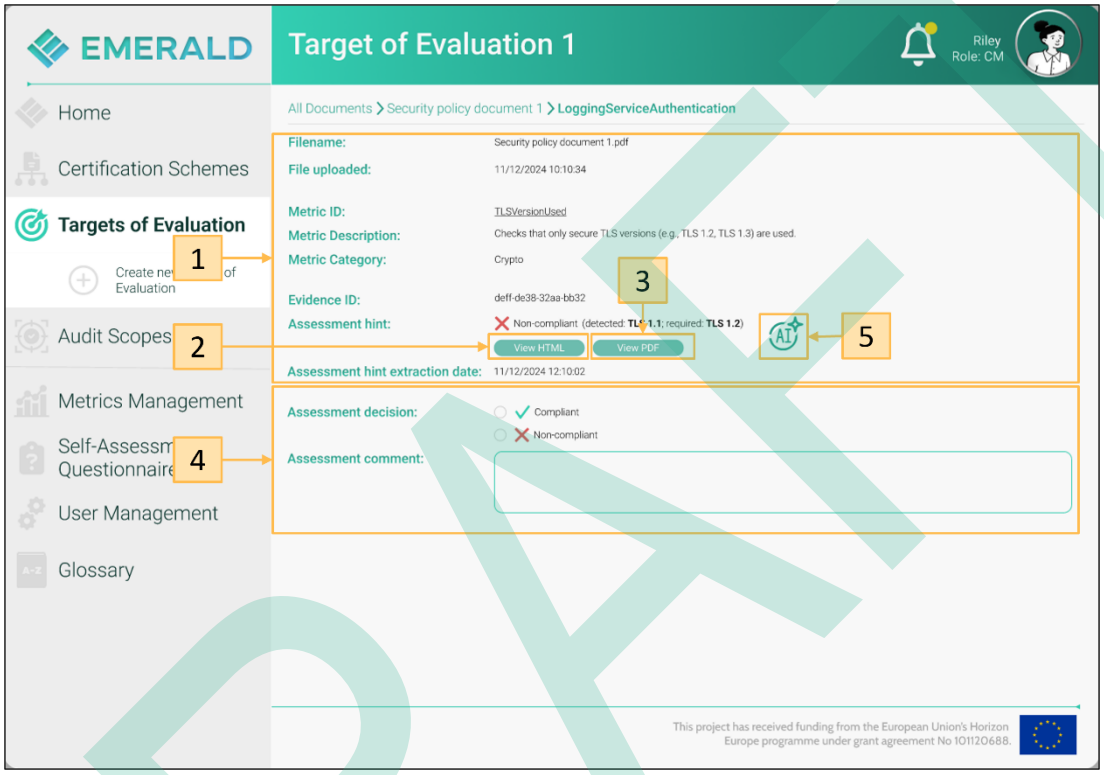

Figure 57. Manage ToE – Security Policy Document Metric View

When clicking on the “Resource” tab (see Figure 58, point 1), the certification graph for the technical evidence will be shown (see Figure 58, point 2). For each resource, all properties and collected evidence can be displayed when clicking on the resource. A user can also view the same information in the form of a table as presented in Figure 59 (Figure 58, point 3).

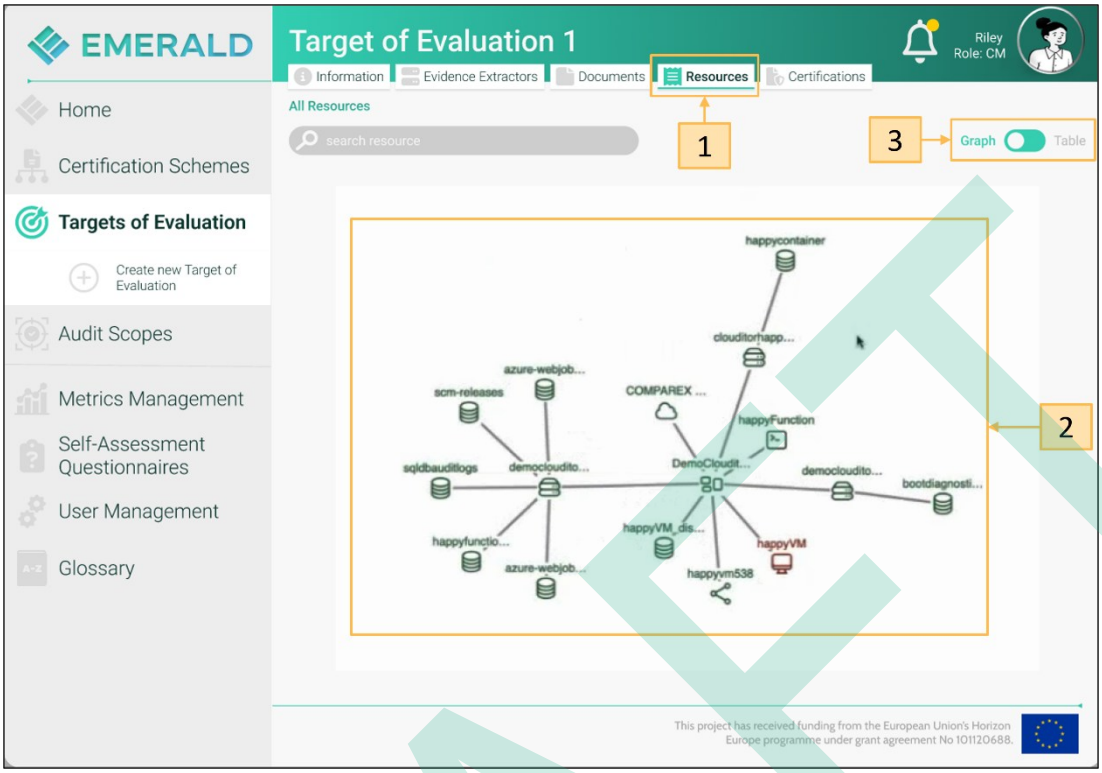

Figure 58. Manage ToE – Resource Graph

The table view presents more information about each resource, namely the assessment status, the resource name, the resource type, the number of metrics extracted, and the date and time when the last evidence was extracted.

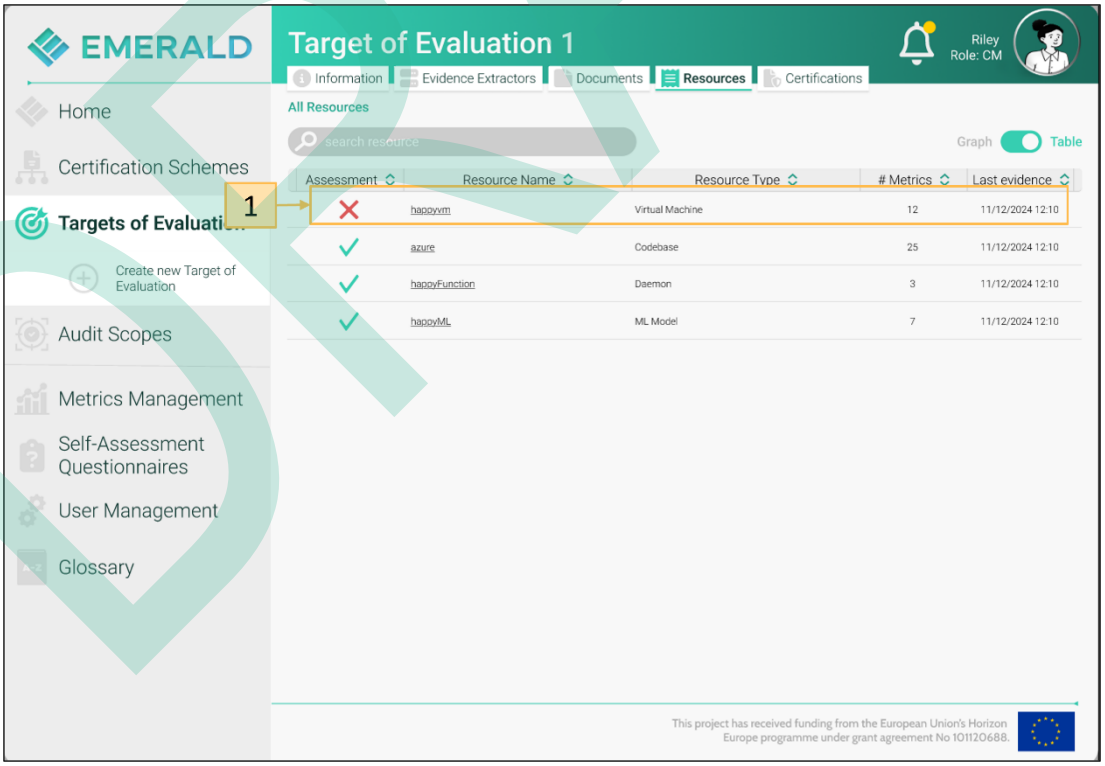

Figure 59. Manage ToE – Resources in a Table view

If a resource is marked in red – independent of the view - the assessment result of a metric is not compliant. In both views – when clicking on the red marked resource, a user gets deeper insights about the metrics and its non-compliance status as presented in Figure 60.

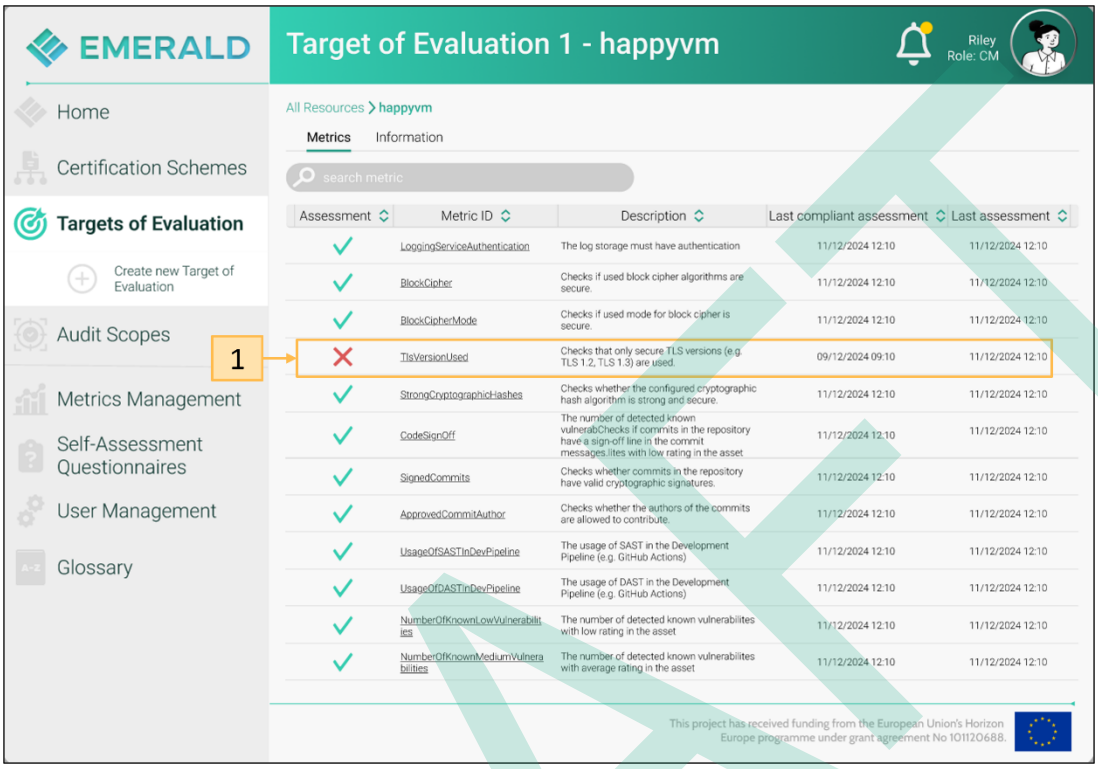

Figure 60. Manage ToE – Assessment Results per Metric

When clicking on the metric marked with a red cross (see Figure 60, point 1), detailed information about why the assessment result is not compliant, is shown in Figure 61.

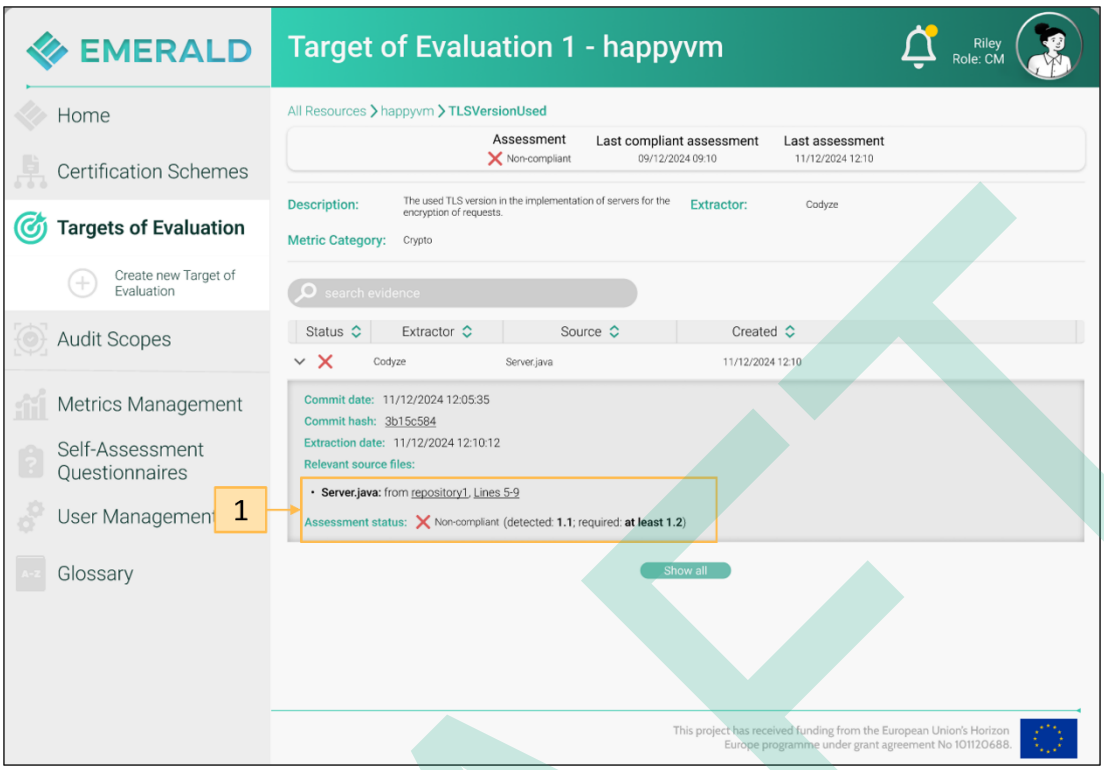

Figure 61. Manage Toe – Show detailed Assessment Result of a Metric

When clicking on the "Certification" tab (see Figure 62, point 1), a user can see all related certifications that have been issued and uploaded. Additionally, a user can upload new certificates (see Figure 62, point 2) and can view already uploaded certificates (see Figure 62, point 3). Additionally, the user gets an overview in which audit scope the ToE is used and has been certified (see Figure 62, point 4).

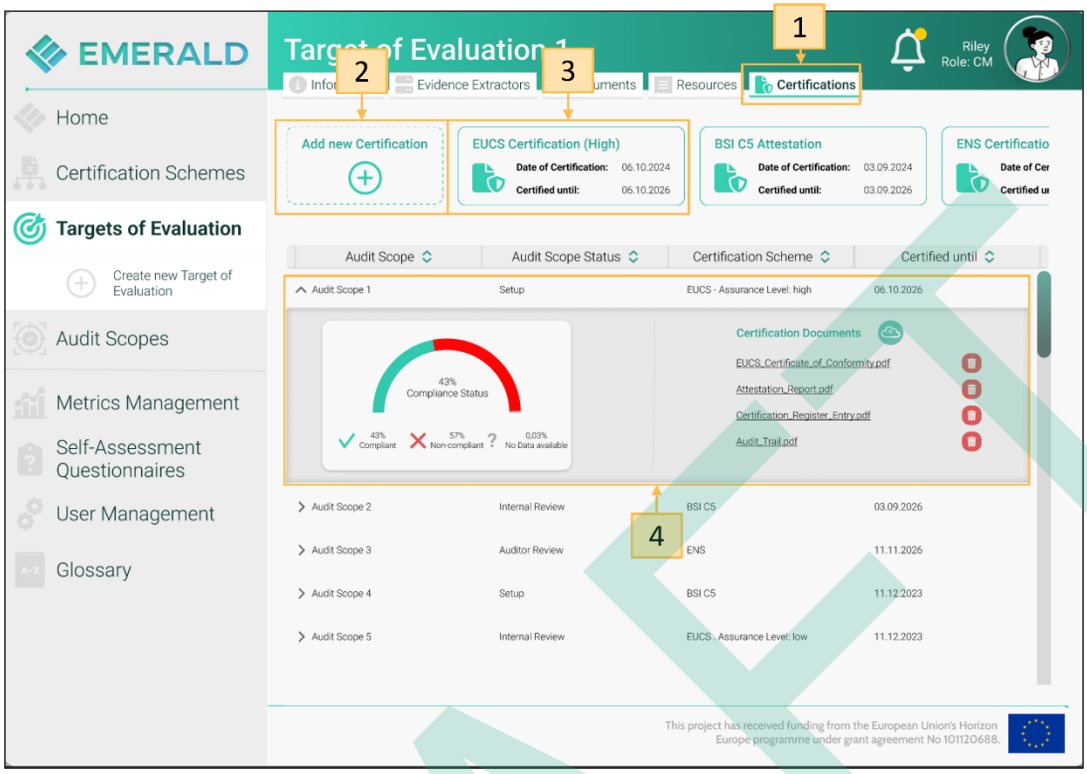

Figure 62. Manage ToE – Certifications

4.5 Setup and Manage Audit Scopes

Stream 3: Setting up and managing audit scopes involves defining, organizing, and overseeing the implementation of controls. To create an audit scope, a target of certification and a certification scheme are selected. Afterwards, user access can be granted to different users. Then the audit scope is set up in EMERALD.

When entering an audit scope, a user can manage the compliance of all controls based on the metrics, assessment results, and evidence retrieved from the evidence extractors (e.g., AMOE; Clouditor-Orchestrator, etc.). Additionally, controls can be assigned to different people. The user can also adapt some general information about the audit scope, as well as the audit scope status. Over more, the user can adapt the scope of the selected certification scheme (e.g., by adding or removing different metrics). If the audit scope covers the EUCS certification scheme, a self-assessment questionnaire can be created. Additionally, reports to export audit information from EMERALD are available.

Figure 63 provides an overview of the actions a user can perform in the audit scope visualisation stream.

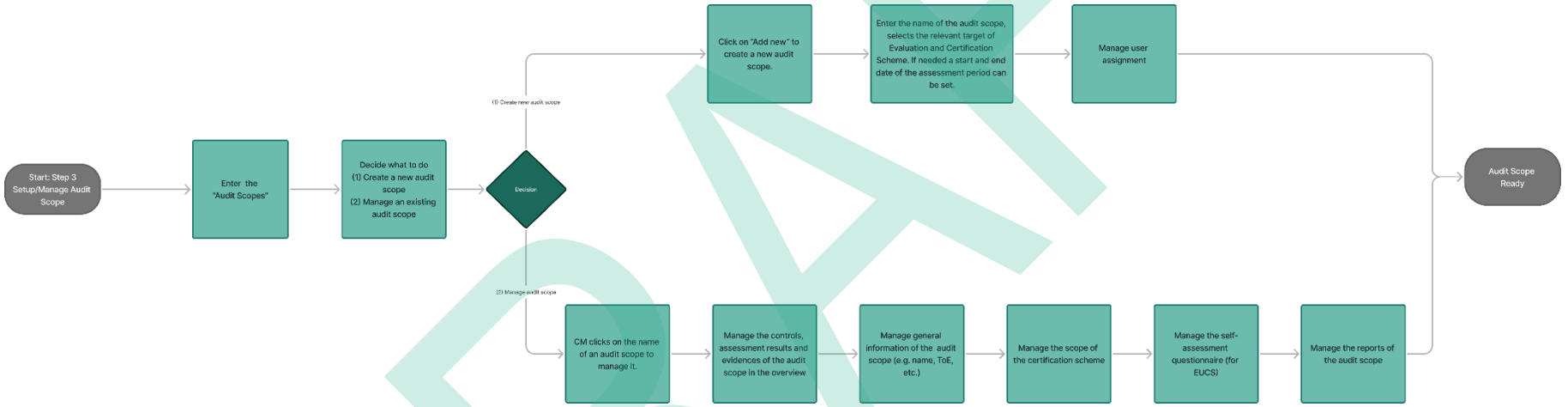

Figure 63. Setup and Management of the Audit Scope Process in the EMERALD UI

4.5.1 Overall Audit Scope Process

Before we present the audit scope views in detail, we are going to present the process flow that guided the development of the audit scope interaction concept.

In order to prepare an audit thoroughly, a concrete process needs to be followed, as shown in Figure 64. This process consists of four different states an audit scope can be in. To support different focus areas during the audit process, two distinct views are available. The "process view" is used to manage all controls along a workflow process. Figure 64 (grey box) presents the different workflow states, their icons, and a concise description of each. The "compliance view" helps to check and track the compliance status of the respective controls. The following sections explain the different states and outline the available actions for each status in the various views.

- **Audit Status 1: Setup**: If an audit scope is in the setup status, typically, the "process view" is the default view. This view shows the status of the control implementation by presenting the workflow status of the controls, as presented in Figure 68. A control can be in the following four different workflow states:
    - Open: This control needs to be dealt with
    - In Progress: Someone is working with this control
    - Implemented: Someone has implemented the control, and a CM needs to check if the control has been correctly implemented
    - Ready for review: This indicates that a CM has verified the control, and it is now ready for final review by the CISO.
    - Accepted: This workflow status is relevant for the next audit scope status "Internal Review".

  At the end of the setup phase, all controls should be set to the status "Ready for Review".
- **Audit Status 2: Internal Review**: If an audit scope is in the internal review status, first, the "process view" is the default view. In this view, the CISO or internal auditor does the final internal review and sets all controls that have been ready for review, after a check to accepted.
    - Accepted: The control and its implementation have been accepted by the CISO, and it can be internally or externally reviewed.

  Then, the CISO or internal auditor switches to the "compliance view". The compliance view shows the overall compliance status of the controls (compliant, non-compliant, or pending) as presented in Figure 71. The CISO checks the non-compliant controls and sets them manually to compliant, if this is possible or necessary. Additionally, the CISO checks non-applicable controls to find out if they are now applicable and can be manually checked with an additional justification.
- **Audit Status 3: External Review**: If an audit scope is in the external review status, the "compliance view" is the default view. The external review takes place; thus, external auditors check the compliance and non-compliance of all the controls.
- **Audit Status 4: Continuous Audit**: If an audit scope is in the continuous audit status, the "compliance view" is the default view. In this phase, the compliance status of all the controls is continuously tracked.

The third view that is available in the audit scope is the "Overall View". This view provides a combined view of the workflow status and the compliance status of the controls. The user can switch between the views whenever needed.

Be aware that changing the audit scope status can only be done by the (Expert) CM of an audit scope. However, the (Expert) CM is allowed to change the audit scope status whenever a change is needed.

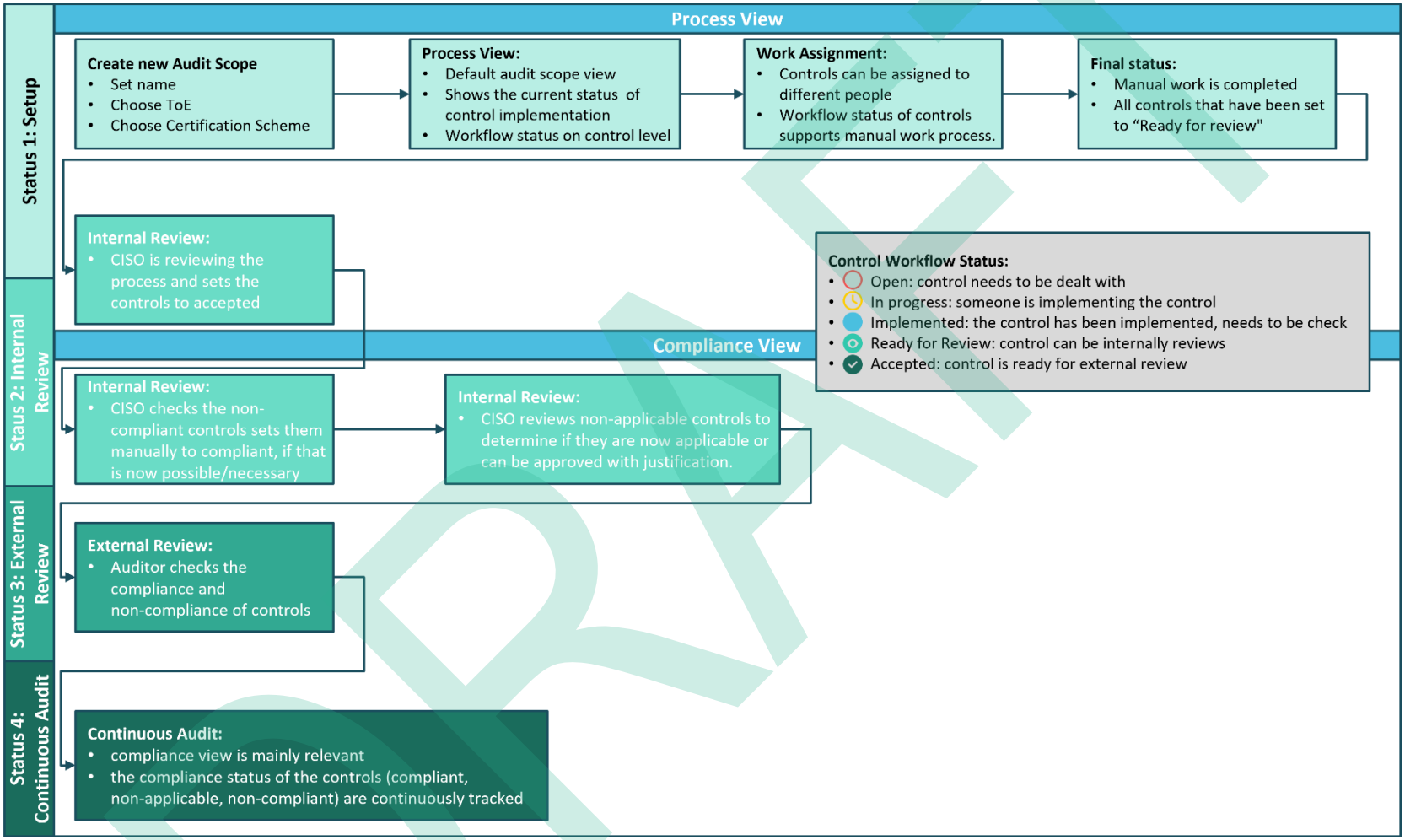

Figure 64. Audit Scope – Status Overview

When entering the audit scope section in the EMERALD UI, a list of audit scopes is presented (in line with the access rights of the user) as shown in Figure 65. Figure 65, point 2, presents the audit scopes that the current user is allowed to see. For each audit scope, one can see the related ToE and the respective certification scheme. Additionally, one can see the workflow status showing how many of the controls of the audit scope are in which state. The compliance status is presented, showing how many controls are compliant or non-compliant. Finally, the overall audit scope status is presented.

Figure 65. Audit Scopes Overview

4.5.2 Setup Audit Scopes

When clicking on “Create new Audit Scope” on the left side (see Figure 65, point 1), the current user can create a new audit scope. Figure 66 presents the first step of setting up a new audit scope. Figure 66, point 1, presents the two steps that need to be fulfilled to set up a new audit scope. In the first step, a user enters a name (Figure 66, point 2), selects an existing target of evaluation (Figure 66, point 3), and selects the respective certification scheme (Figure 66, point 4. After clicking “Next” the user is guided to the user assignment page (see Figure 67).

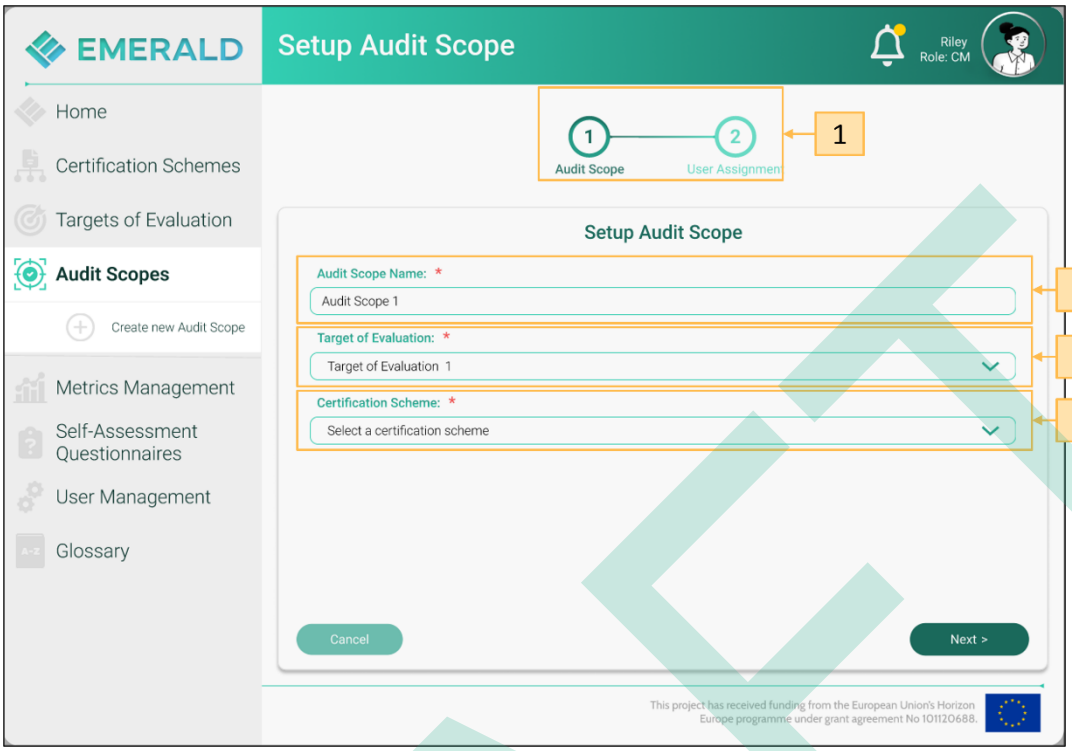

Figure 66. Setup Audit Scope – Step 1 – General Information

In the second step, user assignments can be managed as presented in Figure 67. Figure 67, point 1 allows to search for a user. Below is a list of all users in the EMERALD instance. For each user, one sees if the user has access to the current audit scope, the name of the user, and the role (Figure 67, point 2). Clicking “Save” (Figure 67, point 3) creates the new audit scope.

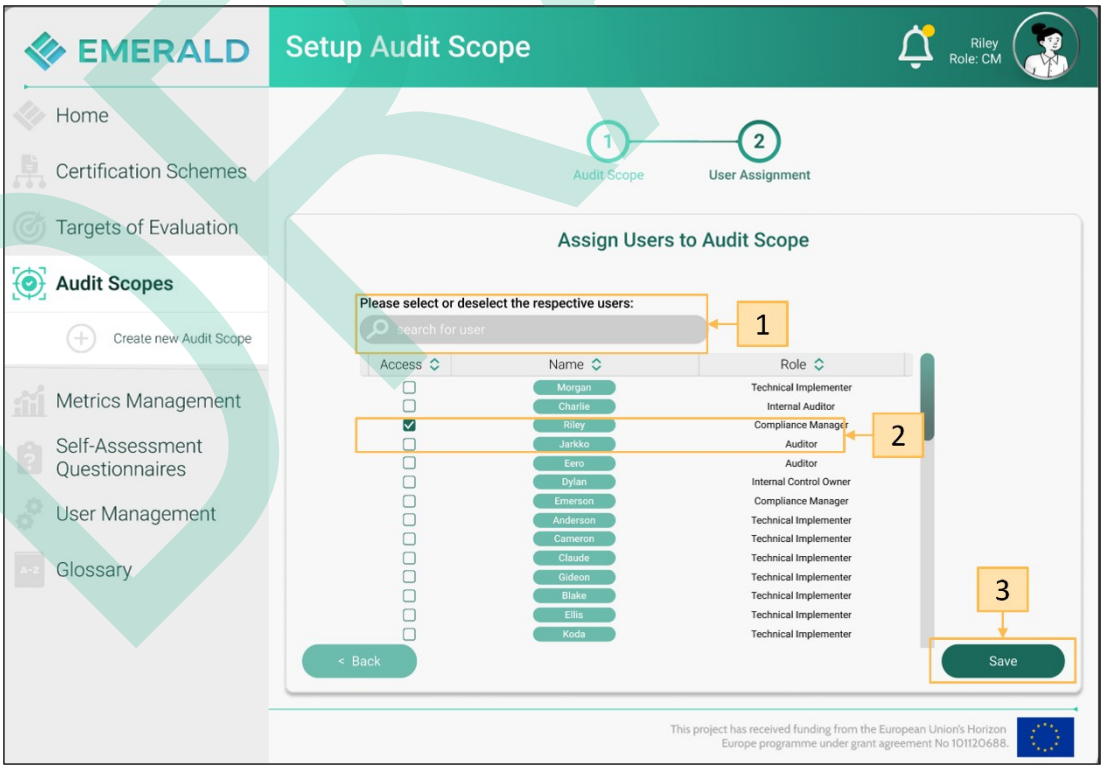

Figure 67. Setup Audit Scope – Step 2 – User Assignment

4.5.3 Manage Audit Scopes

After having created a new audit scope, a user has the possibility to manage it. Therefore, the user needs to click on the name of the audit scope like for example, “Audit Scope 1” in the overview page (see Figure 65).

When entering an audit scope, the following view is presented as shown in Figure 68. Using the tabs in Figure 68, point 1 allows a user to go through the submenu; these include the overview, general information about the audit scope, the scope selection to adjust the certification scheme, the self-assessment questionnaire (if the certification scheme of the audit scope is EUCS), and the reports.

Each of the tabs will be presented in detail: the overview tab (see Section 4.5.3.1), the general information tab (see Section 4.5.3.1), the scope selection tab (see Section 4.5.3.2), the self-assessment questionnaire tab (see Section 4.5.3.3), and the reports tab (see Section 4.5.3.4).

4.5.3.1 Overview Tab

Figure 68 presenting the overview tab is described briefly. Then, we present each functionality available in this view in more detail along the bullet point list below.

- **Audit Scope Information**: Figure 68, point 2 provides the general information about the audit scope, namely the related ToE, the selected security scheme (and assurance level if the scheme is EUCS), the current audit scope status, and an edit button (for details see Figure 69).
- **Audit Scope - TWS**: Figure 68, point 3 shows the result of the *TWS* (see Figure 70).
- **Audit Scope - Process view, compliance view, overall view**: Figure 68, point 4 allows to switch between the different views: the process view – shown when the audit scope status is setup or internal review (see Figure 68), the compliance view – shown when the audit scope status is external review or continuous compliance (see Figure 71), and the overall view – combining insights from both views (see Figure 72).
- **Audit Scope - Control workflow overview and details**: Figure 68, point 5 displays the control workflow overview as percentages, indicating how many controls fall into each workflow status Figure 68, point 6 presents how many controls in which status is assigned to the current user (Assigned to me – left column) from all available controls (All controls – right column) By clicking on the numbers, a user can filter for controls in the respective status.
- **Audit Scope - Search bar**: Figure 68, point 7 allows searching for different categories and controls.
- **Audit Scope - Categories and Controls of certification scheme:** Figure 68, point 9, presents the status of the categories and controls hierarchically. By clicking on the categories, one can browse to the individual control. For the categories of a scheme, an aggregated status is presented of the underlying controls. When having opened a category and a sub-ordinated category, the respective controls and the controls individual workflow status are presented. By clicking on the control name, a user gets more information about the control, as shown in Figure 74. Figure 68, point 8 allows switching between the hierarchical view of categories and controls (shown in Figure 68) and a flat view of the individual controls.

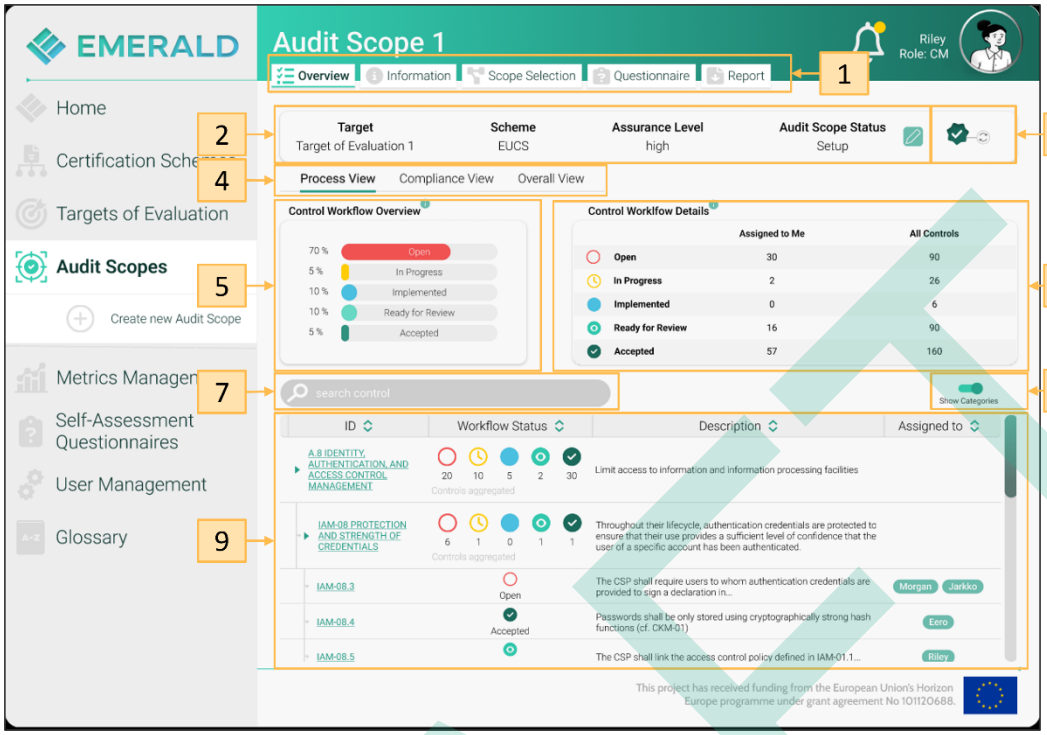

Figure 68. Manage Audit Scope – Overview

Audit Scope Information: Figure 68, point 2, provides the general information about the audit scope. When clicking on the Edit button, the following pop-up opens as shown in Figure 69. On top of Figure 69, point 1, a user sees the certification scheme and ToE selected – this information cannot be changed. A user can change the name of the audit scope (Figure 69, point 2), the audit scope status (depending on user rights; Figure 69, point 3), and assign a new audit scope owner (Figure 69, point 4). When clicking on the "Save button", all changes will be stored (Figure 69, point 5).

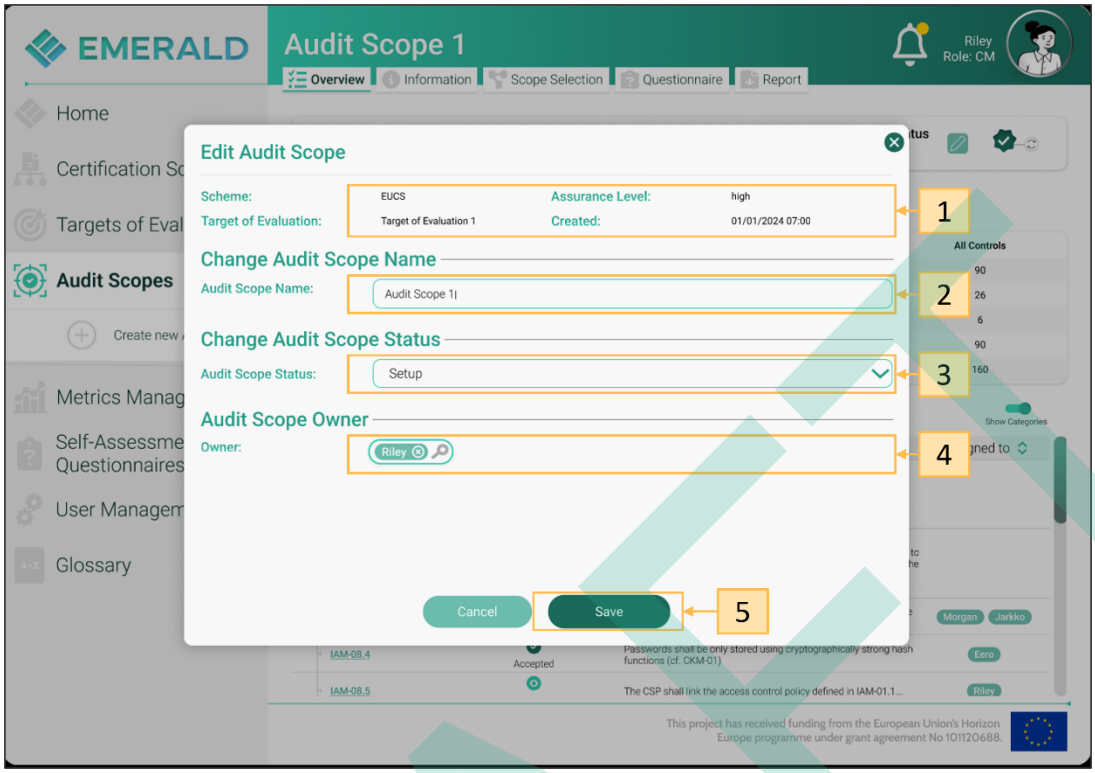

Figure 69. Manage Audit Scope – Edit an Audit Scope

Audit Scope: *TWS*: Figure 68, point 3, shows the result of the integrity check provided by the *TWS*. If the integrity check is ok, a green symbol is presented (Figure 68, point 3). If the integrity check fails, the green symbol turns into a red symbol (see Figure 70, not depicted). Additionally, a user can open (Figure 70, point 1) and/or download (Figure 70, point 2) the TWS report to get more information about the failed integrity check.

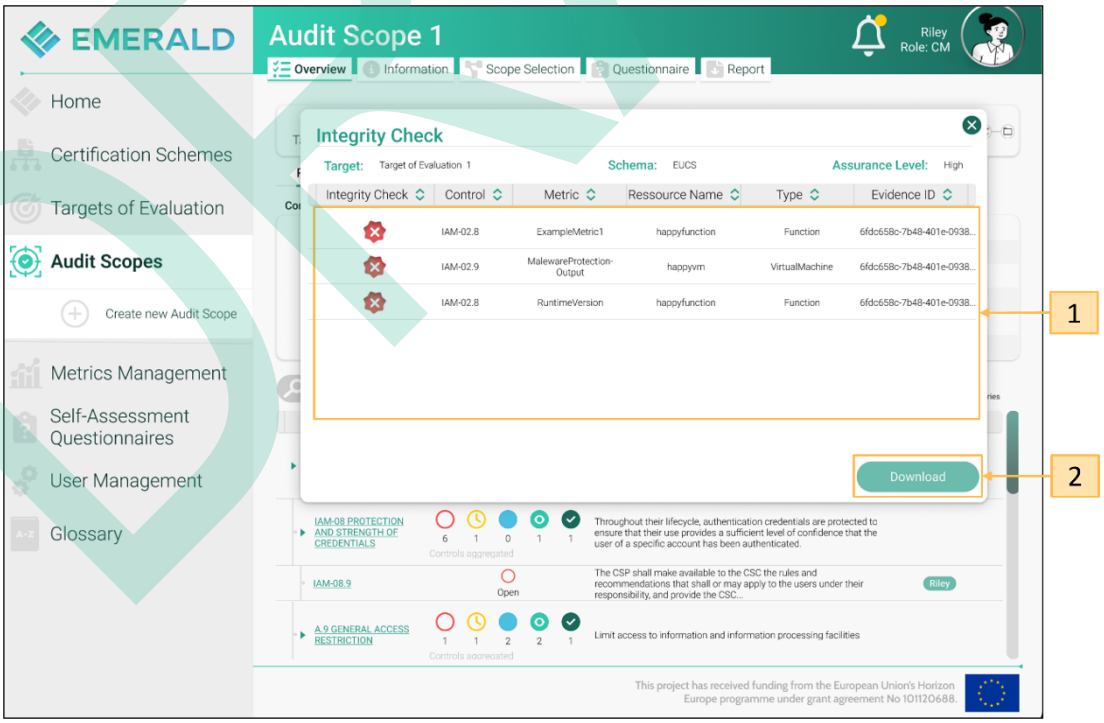

Figure 70. Manage Audit Scope – Integrity Check by TWS failed

Audit Scope: Process view, compliance view, overall view: Figure 68, point 4 allows switching between the different views.

- **Process view**: The process view shown in Figure 68 allows tracking the workflow process states of all controls. This view is used when the audit scope status is either set to "setup" or "internal review". Each control has one of the following states: open, in progress, implemented, ready for review, and accepted (for details, see Section 4.5.1). Regarding the list of categories and controls of the current certification scheme, it presents the categories and controls with the workflow implementation status in a hierarchical way. For example, in Figure 68, point 9 shows that category A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT has below 20 open controls, 10 in progress controls, 5 implemented controls, 2 ready for review controls, and 30 accepted controls. Another example is that it shows that the control "IAM-08.3" is currently "open".
- **Compliance view**: The compliance view is presented in Figure 71. This view is used when the audit scope status is "internal review" (depending on the status of the controls implemented), "external review", and "continuous audit". It shows the overall compliance status of the audit scope. Figure 71, point 1, shows in percentage how many controls are already compliant, how many of them are not compliant, and how many of them are pending. Figure 71, point 2, provides the same information but with absolute numbers and some further subdivision. It shows how many controls have been set automatically to compliant, how many controls have been set manually to compliant, how many controls have been set automatically to non-compliant, how many controls have been set manually to non-compliant, and how many controls are still pending regarding their compliance status. Figure 71, point 3, shows the categories and controls with their compliance status in a hierarchical way. For example, category A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT has 30 compliant controls and 17 non-compliant controls. Another example is that control IAM-08.3 is non-compliant so far.
- **Overall view**: The overall view combines the process view and the compliance view into one view for getting a quick overview (see Figure 72). This view is not related to any status of the audit scope. Figure 72, point 1, shows the detailed view of the workflow status per control of the audit scope. Figure 72, point 2, shows the detailed view of the compliance status of the controls along the 5 types possible. Figure 72, point 3, shows again all categories and controls in a hierarchical way. In this case, a user sees the workflow status as well as the compliance status of categories and controls.

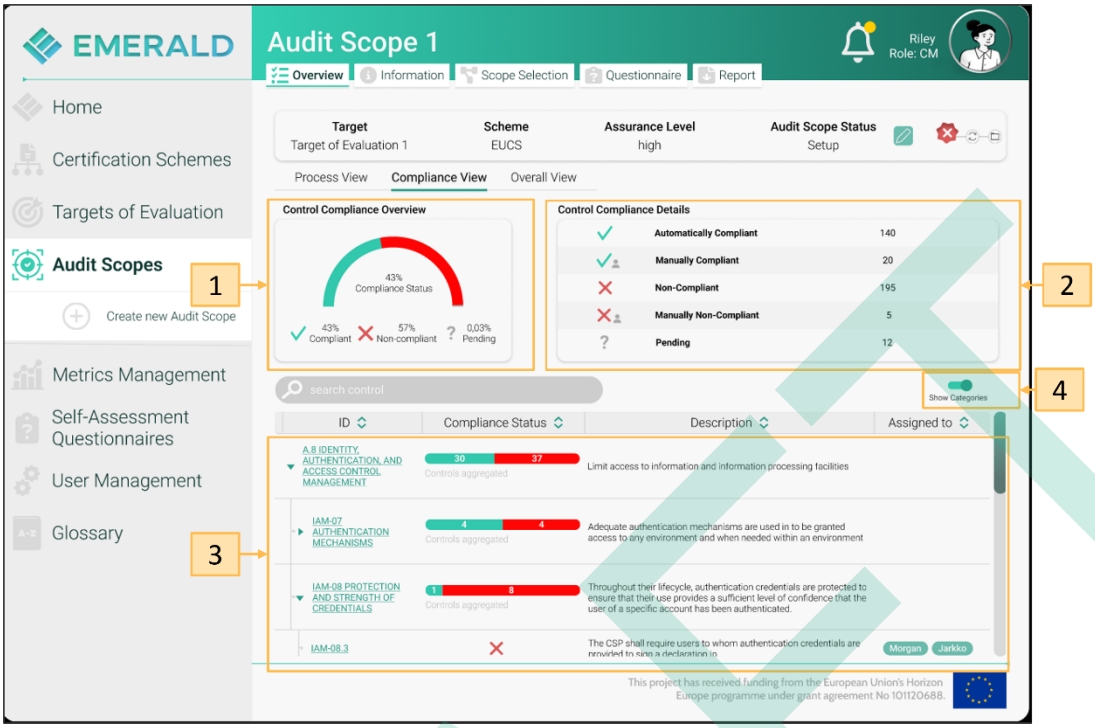

Figure 71. Manage Audit Scope – Compliance View

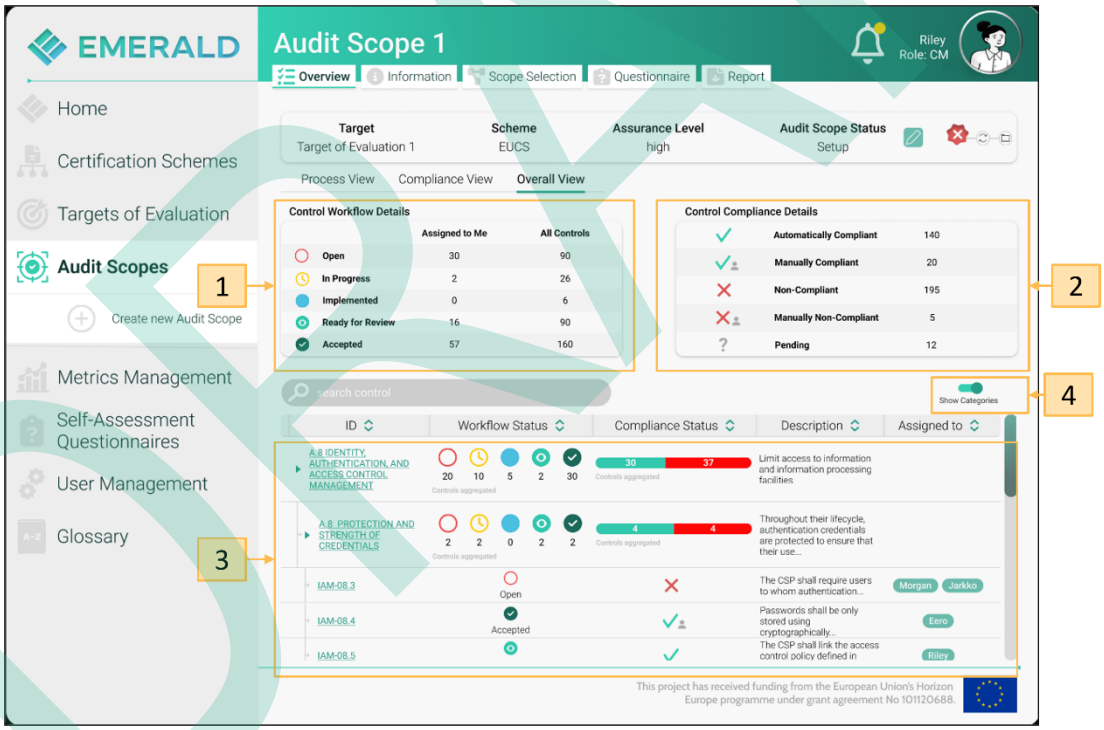

Figure 72. Manage Audit Scope – Overall View

Independent of the views – the process view, the compliance view, and the overall view we presented the categories and controls in a hierarchical way, where a user can click on categories, subordinate controls, until the user reaches the individual controls. All three views offer the option to switch from a hierarchical view to a flat list view, in the process view Figure 68, point 8, in the compliance view Figure 71, point 4, and in the overall view Figure 72, point 4. Exemplarily, we show the flat list view on the basis of the process view (see Figure 73, point 1); for the compliance and the overall view, the flat control list looks similar.

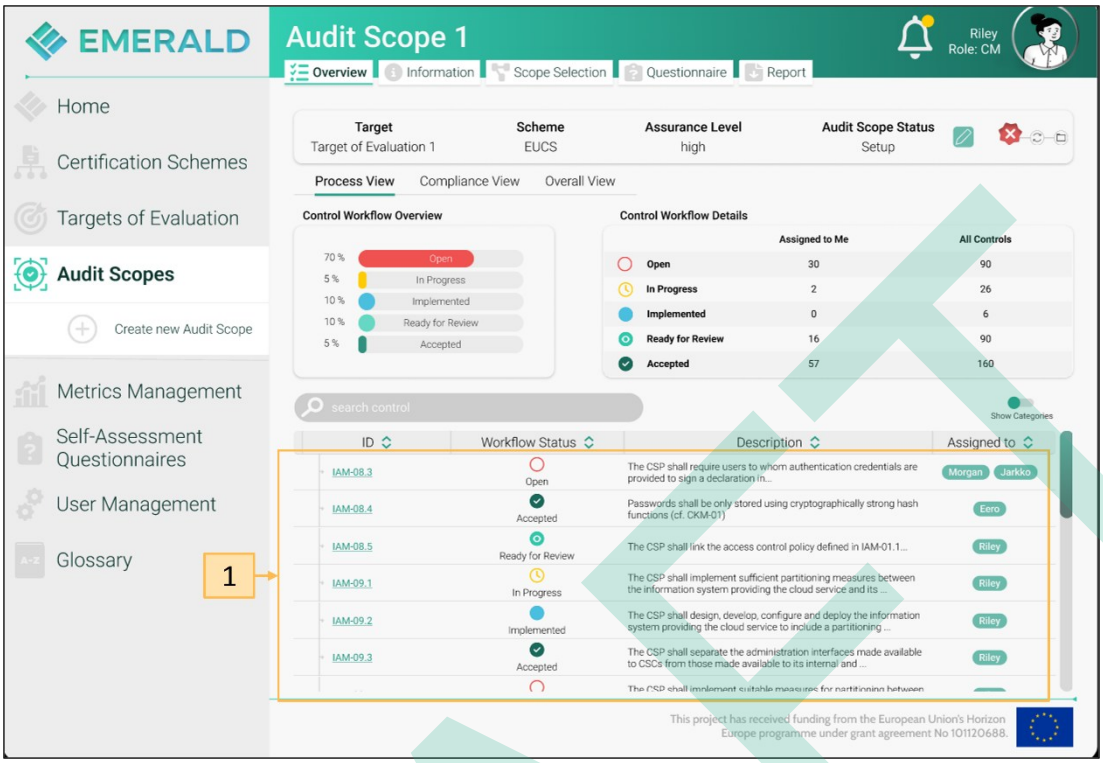

Figure 73. Manage Audit Scope – Process View – Controls in a List

Audit Scope: Categories and Controls of the certification scheme:

To get further insights about a control e.g., why a control is marked as open, the user needs to click on the name of the control, like for example in Figure 68, point 9, and control IAM-08.3. Then the user sees the following control view as presented in Figure 74. First, Figure 74 is described briefly. Second, we present each functionality available in this view in more detail along the bullet point list below.

- **Control: Navigation**: On top of Figure 74, point 1, the user sees the name of the control and the related audit scope. When clicking on the name of the audit scope, the user is redirected to the overview of the audit scope (to Figure 68).
- **Control: Control properties**: Figure 74, point 2 provides more information about the control itself, for example, the compliance status, the workflow status, to whom the control is assigned, and the owner of the control. When clicking on “More details" the user gets information about the date and time when the control was updated and until when the manual compliance is valid (if applicable). Also, some of the control properties can be edited as presented in Figure 75.
- **Control: Further Control Information**: Similar to the audit scope, there is also the possibility to switch between different views in the control overview. In the assessment views (shown in Figure 74, point 3) a user sees the assessment results. In the information view, the user can access the description of the current control provided by the respective certification scheme (see Figure 76). Finally, a user can access the history of a control, showing which user did what with respect to the control (see Figure 77).
- **Control: Control Metrics List**: Figure 74, point 4 presents the list of metrics that have been assigned to the control. For each metric, the assessment status, the name of the metric, the description of the metric, the last compliant evidence extracted, and the last evidence extracted are shown. Additionally, a user can still decide on the applicability of the different metrics. For example, in the third line of Figure 74, point 4, it shows that

the assessment result of the “ExampleMetric2” is not ok, while the assessment results for the other three metrics are fine.

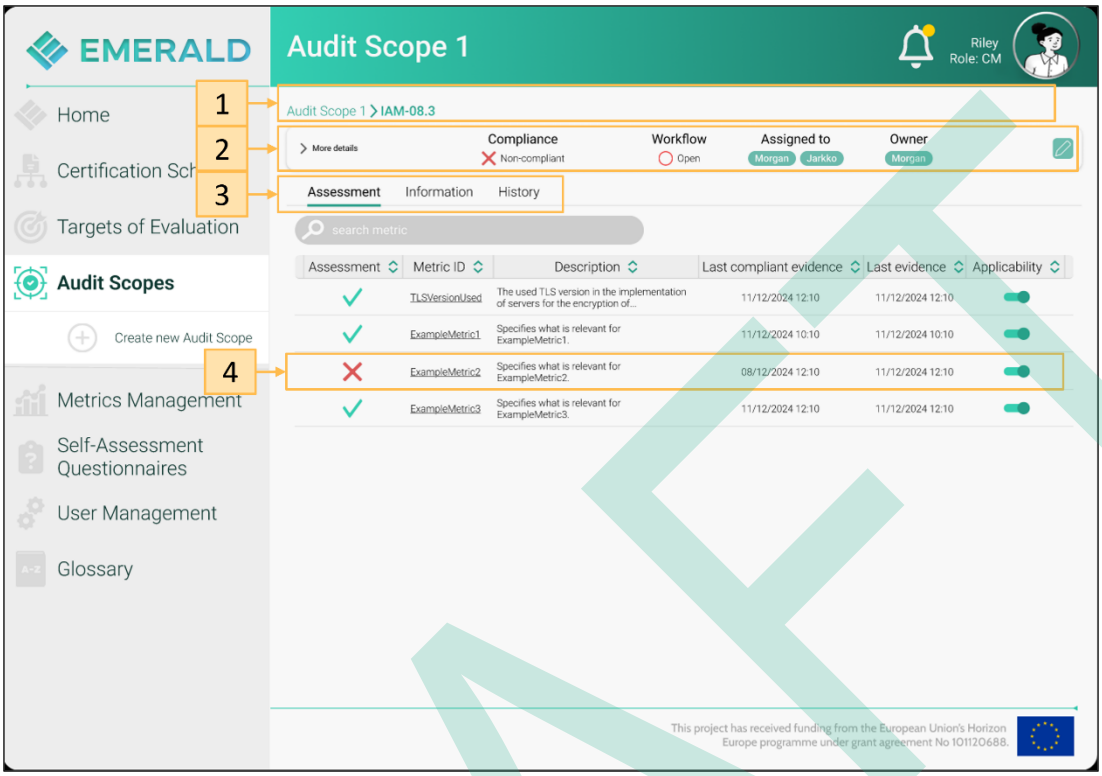

Figure 74. Manage Audit Scope – Enter a Control

Control: Control properties

When clicking on the edit button, Figure 74, point 2 on the right side, the user is able to change some relevant properties of the control, as shown in Figure 75. For example, the user can manually adjust the compliance status (see Figure 75, point 1), the user can change the workflow status of the control (see Figure 75, point 2), the user can assign the control to another person or department (see Figure 75, point 3), and the user can also change the owner of the control (see Figure 75, point 4).

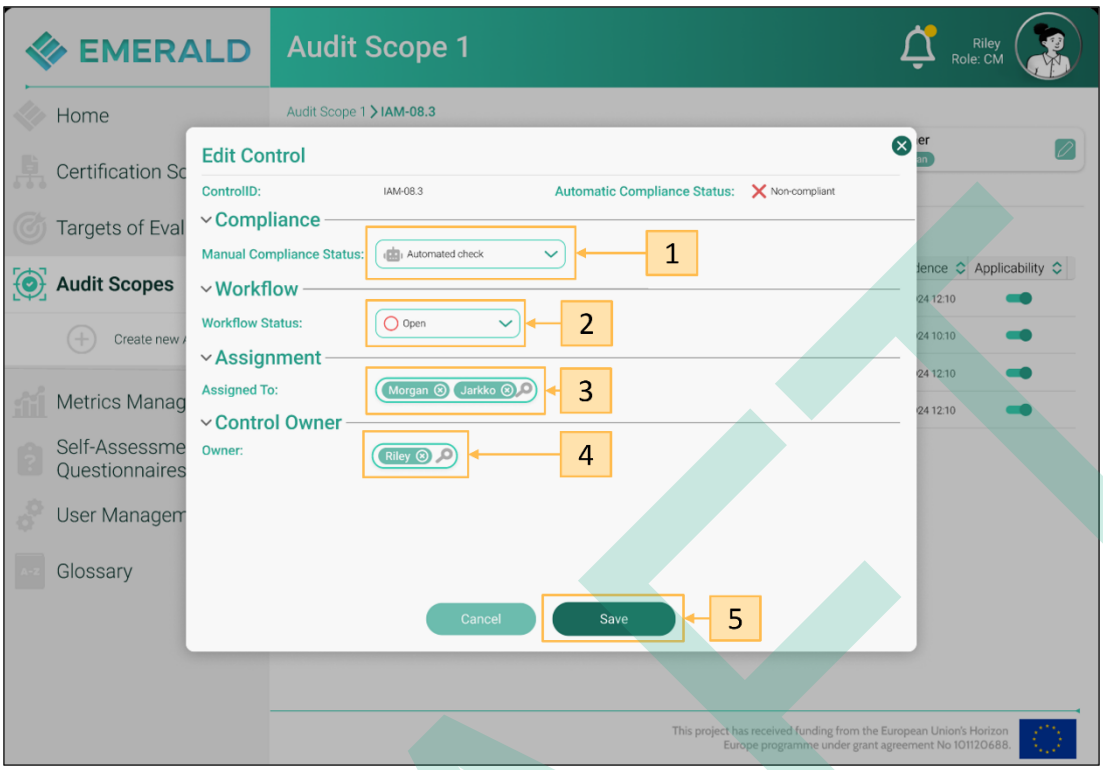

Figure 75. Audit Scope – Control – Edit Control Properties

Control: Further control information: Figure 74, point 3, shows that further information about a control is available. When the "Assessment" tab is active, the assessment results per metric are shown (see Figure 74).

Clicking on the "Information" tab (see Figure 76 point 1), further information about the control is shown, namely, to which certification scheme, which category, and sub-ordinate category it belongs. If an implementation guideline for the control is available, then it will also be presented in this view.

Switching to the "History" tab (see Figure 77), the view presents the history of the control. It shows which actions were conducted, which changes were made, by whom, and when. This enables monitoring the progress of the control over time.

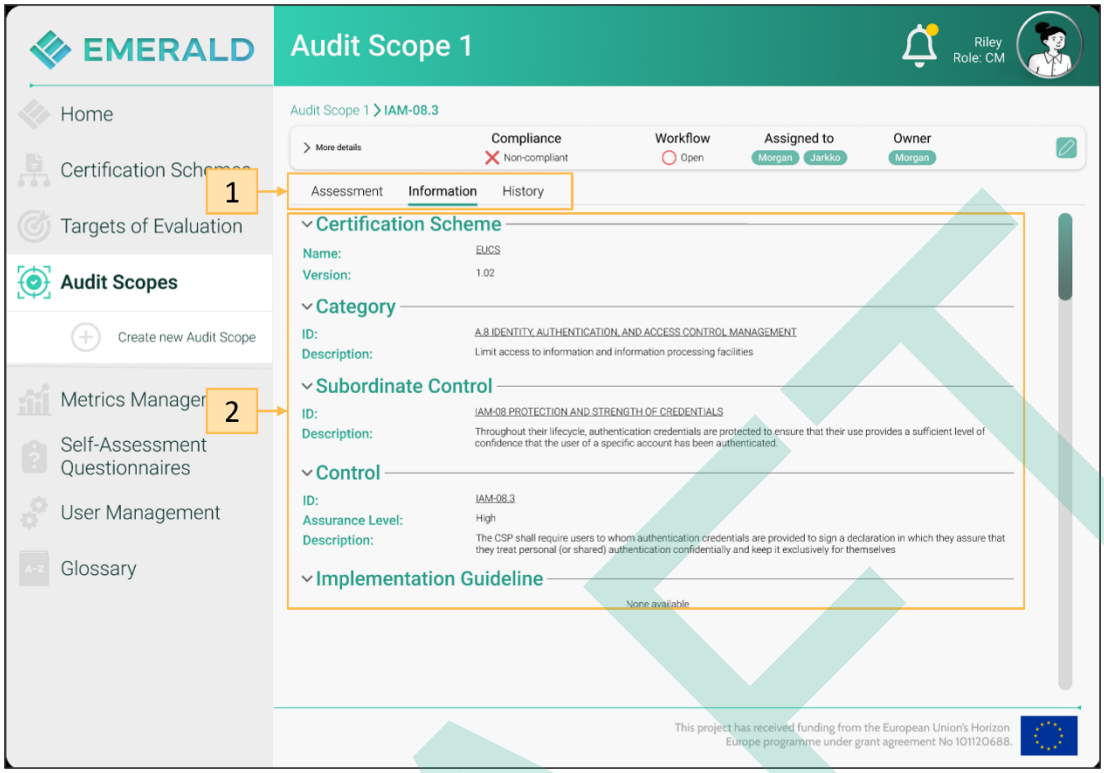

Figure 76. Audit Scope – Control – Further Information

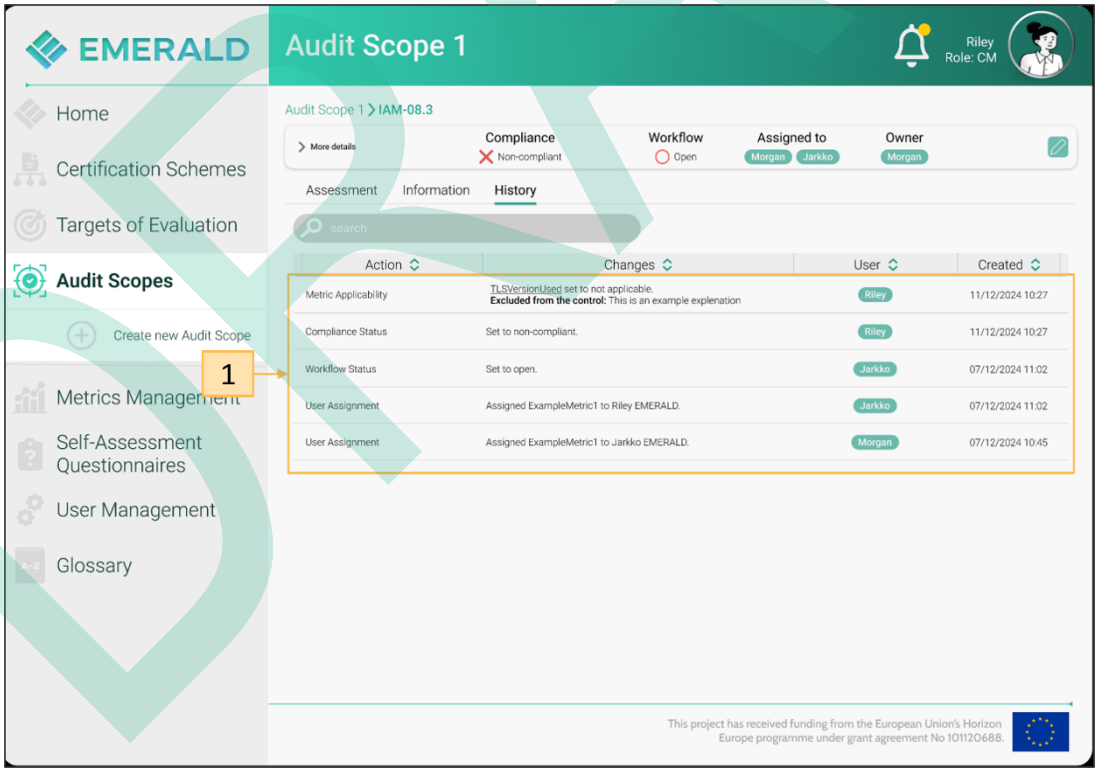

Figure 77. Audit Scope – Control – History

Control: **Control Metrics List:** Figure 74, point 4 presents the list of metrics that have been assigned to the control. For each metric, the assessment status, the name of the metric, the description of the metric, the last compliant evidence extracted, and the last evidence extracted are shown. When clicking on the name of the metric, more information about the metric will be shown as depicted in Figure 78. Figure 78 shows the information about the compliant metric named "TLSVersionUsed". Figure 78, point 1 shows the breadcrumb navigation for the metric – the name of the audit scope, the control, and the name of the metrics, which can be used for navigation. Figure 78, point 2 provides general information about the status of the metric, including the assessment result, the last compliant assessment result retrieved, the last assessment result of the metric retrieved, and its applicability. When clicking on the edit icon, some properties of the metrics can be changed (see Figure 80, point 1) – the operator, the target value, and the target value datatype. Figure 78, point 3 provides more information about the metrics – on the one hand there is a description of the metrics and to which metric category the metric belongs to – on the other hand it presents in which other controls of the current audit scope the metric is used and which evidence extractors (e.g. Codyze, AMOE) are related to the control to extract the assessment result. Figure 78, point 4 shows the assessment results of the evidence extractor Codyze, and Figure 78, point 5 shows the assessment results of the evidence extractor AMOE. In both cases, the assessment status is compliant, indicating that both extractors can provide evidence demonstrating the metric's fulfilment.

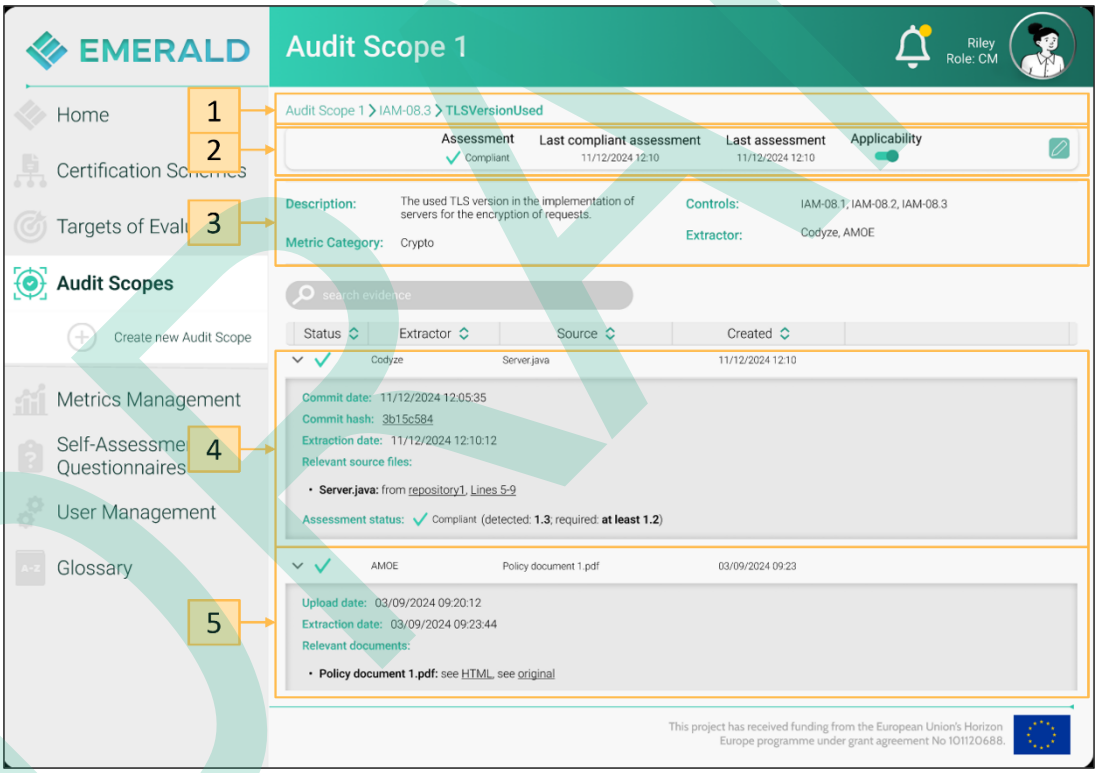

Figure 78. Audit Scope – Control – Metric compliant

Figure 79 shows the same information for another metric "ExampleMetric2". In this case, the assessment result is non-compliant. Having a closer look at Figure 79, point 1 provides more insights about the assessment result of the evidence extractor *eknows-e3*, showing that in the file "repository1" in the lines 5-9, the evidence extracted stated that the logging is disabled instead of being enabled. A user can directly jump to the respective source files to see where the non-compliance is coming from.

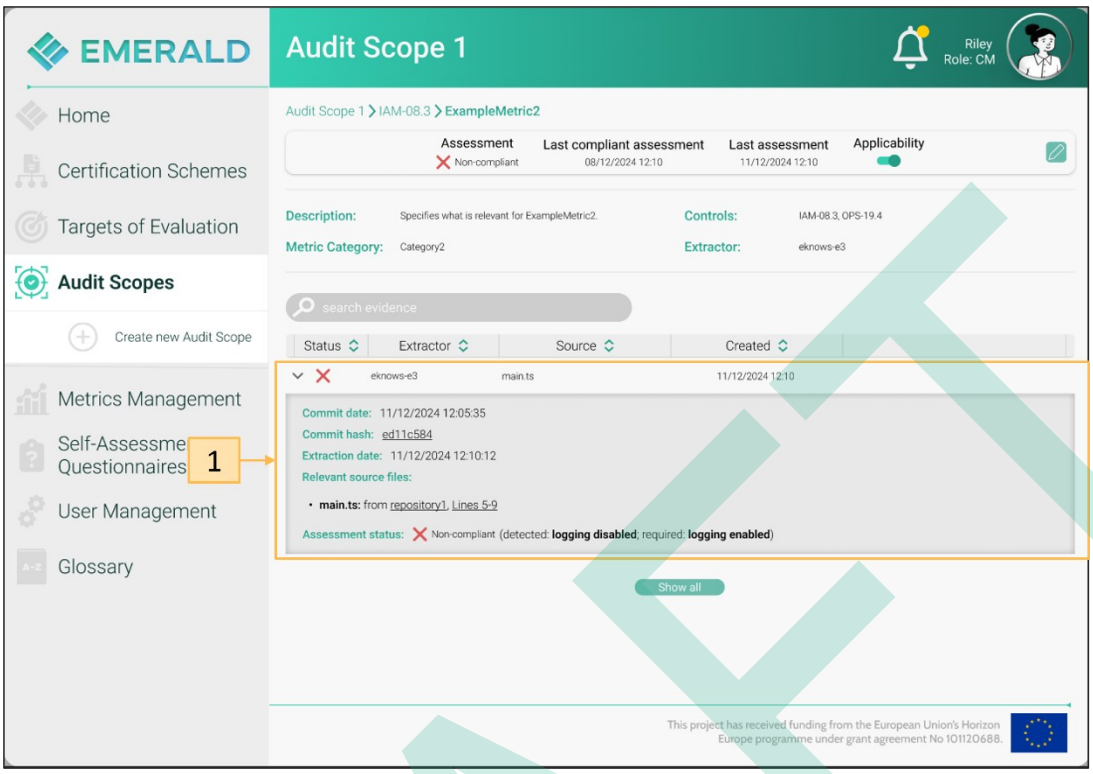

Figure 79. Audit Scope – Control – Metric non-compliant

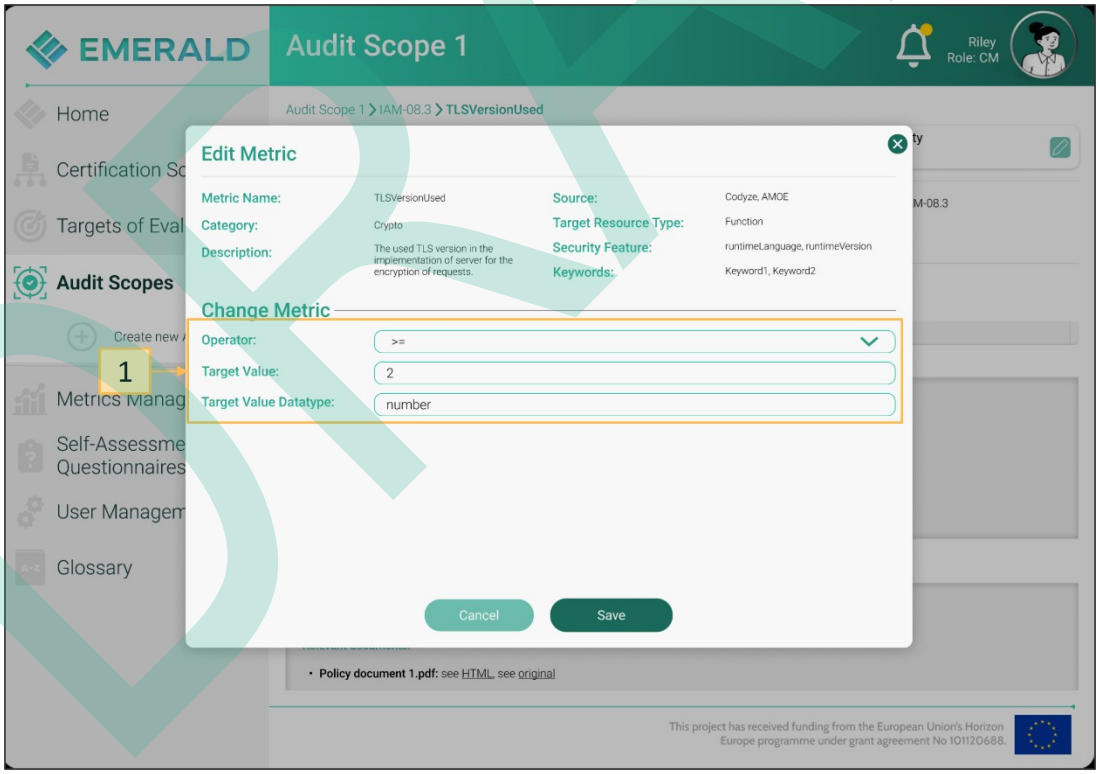

Figure 80. Audit Scope – Control – Edit Metric Properties

Figure 74 above is a representation of how the control view looks if metrics are assigned to a control (in this case, to control IAM-08.3). However, it can also happen that no metrics can be assigned to a control, for example IAM-08.4 (Figure 74). Thus, no assessment result and evidence

can be automatically extracted with the help of an evidence extractor. Therefore, it needs to be possible to manually upload documents that show that a control is fulfilled, as presented in Figure 81. In Figure 81, point 1, a user can add a comment for the control and how evidence is shown so that the control is fulfilled. Clicking on the "Upload" button (Figure 81, point 2), a user can upload respective files. Figure 81, point 3, presents the list of files that have been uploaded to show evidence that the control is fulfilled.

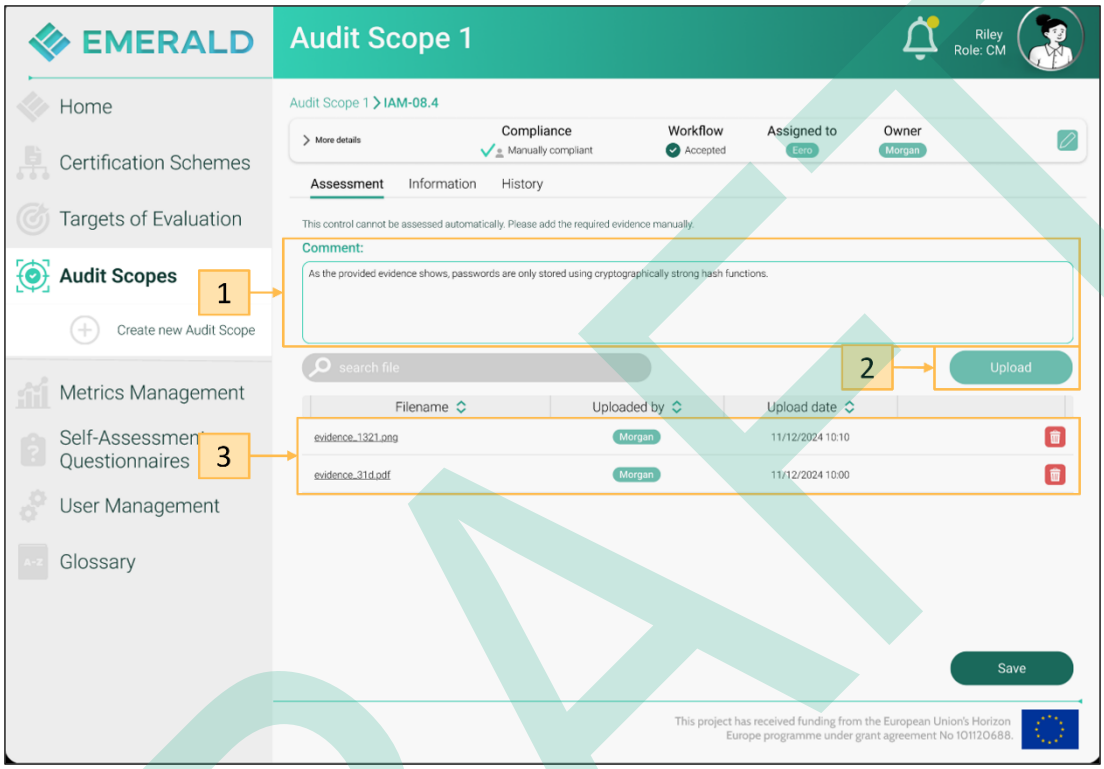

Figure 81. Audit Scope – Control without Metrics

4.5.3.1 Information Tab

The information tab (Figure 82, point 1) presents further information about the audit scope divided into three parts:

- **General**: The general part of the audit scope covers general information about the audit scope (see Figure 82, point 2) like the name of the audit scope, the selected ToE, the selected certification scheme, the creation date, the assessment period with a start and end date, the audit scope status, and the audit scope owner.
- **User assignment**: In the user assignment part (see Figure 82, point 3), all users who are currently assigned to the audit scope are listed.
- **History**: The history part (see Figure 82, point 4) presents all activities and changes that have been done by whom and when in the audit scope.

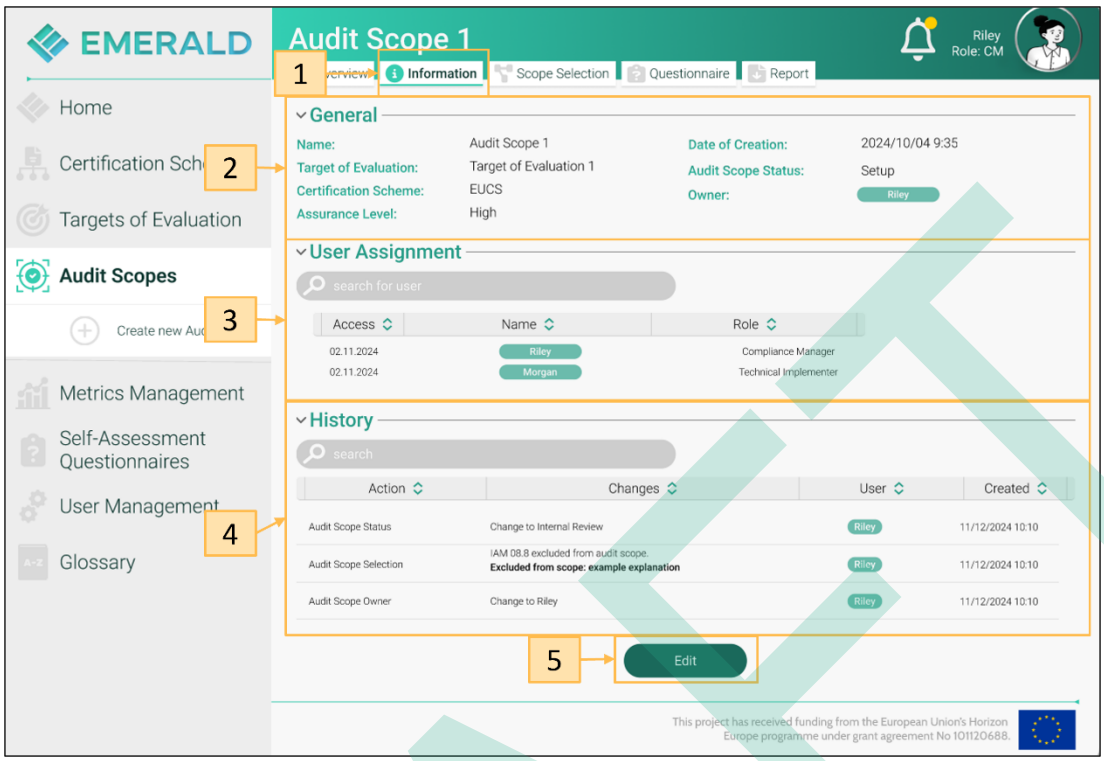

Figure 82. Audit Scope – Information Tab

When clicking on the "Edit" button (Figure 82, point 5), some general information as well as the user assignment can be changed, if a user has the corresponding rights (e.g., CM or Expert CM). Figure 83, point 1 shows that a user is allowed to change the name of the audit scope, the start and end date of the assessment duration, the audit scope status, and the audit scope owner. Figure 83, point 2 shows that a user is also allowed to manage the access rights, thus, grant access to further users or remove users' access rights.

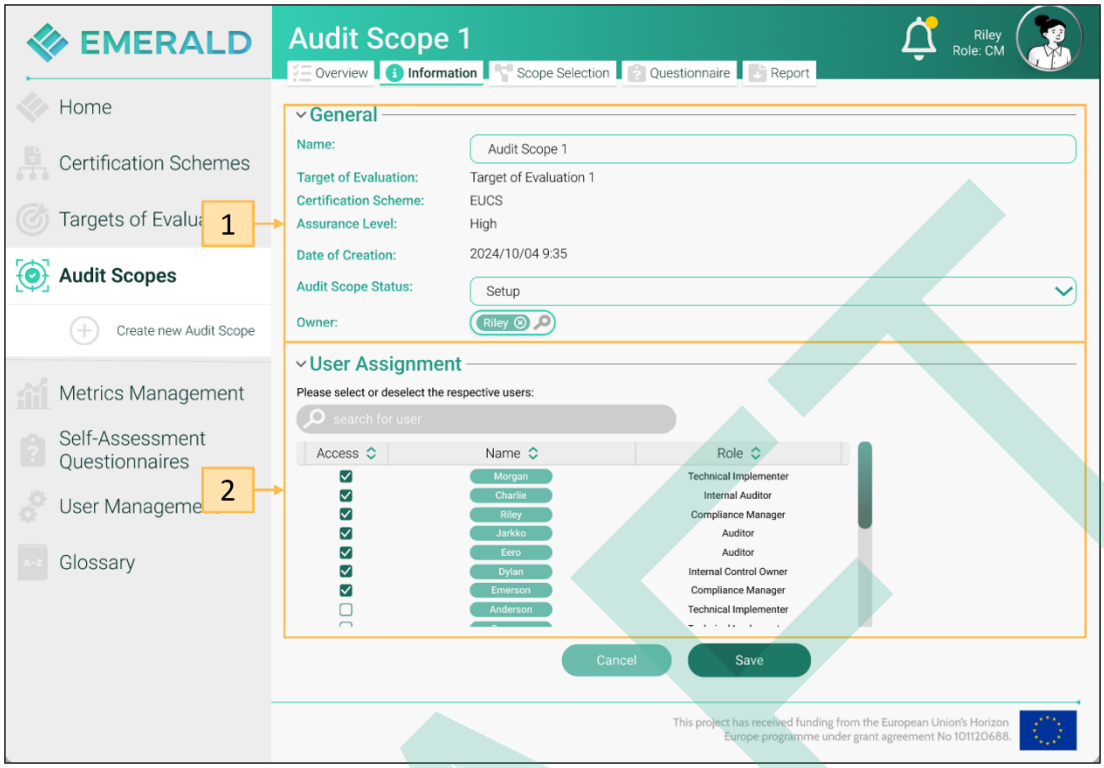

Figure 83. Audit Scope – Information Tab – Edit

4.5.3.2 Scope Selection Tab

The scope selection tab (see Figure 84, point 1) presents the current certification scheme, including the categories and controls applicable for the current audit scope. Figure 84, point 2, shows the certification scheme in a hierarchical view, the checkbox on the right indicates that the respective category and control are applicable for the current audit scope.

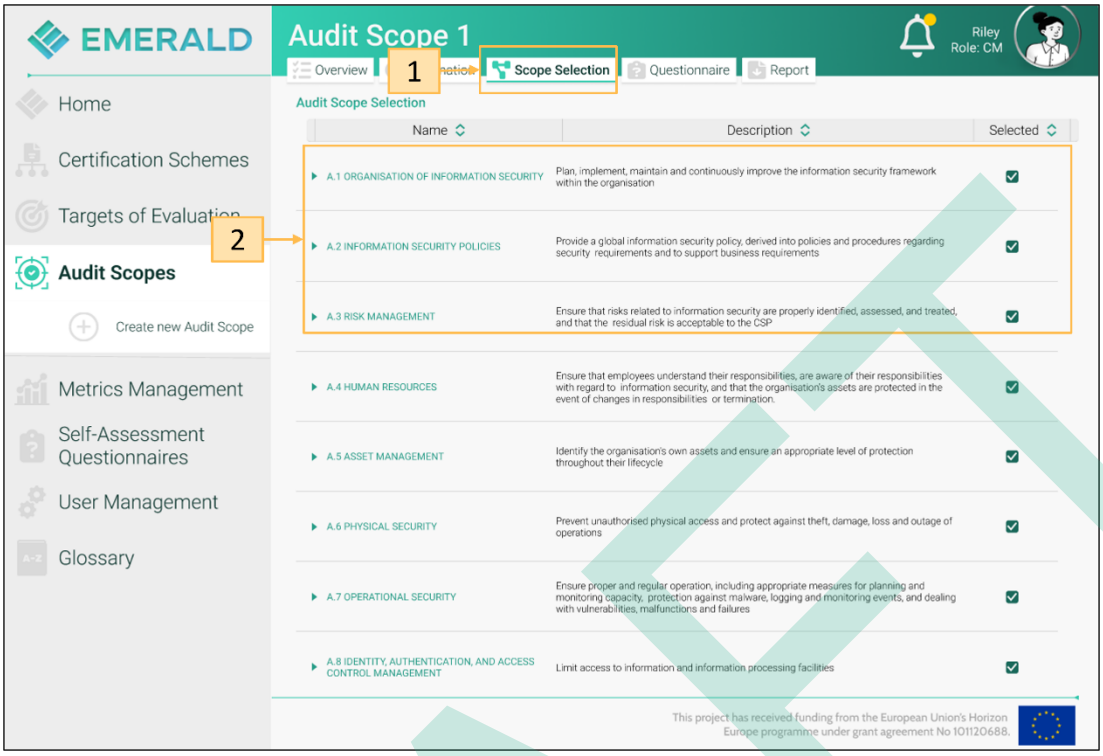

Figure 84. Audit Scope – Scope Selection Tab – Overview

When deselecting a complete category – as shown in Figure 85, point 1 – a pop-up window shows up, Figure 85, point 2, asking to provide some explanation why the category will be removed.

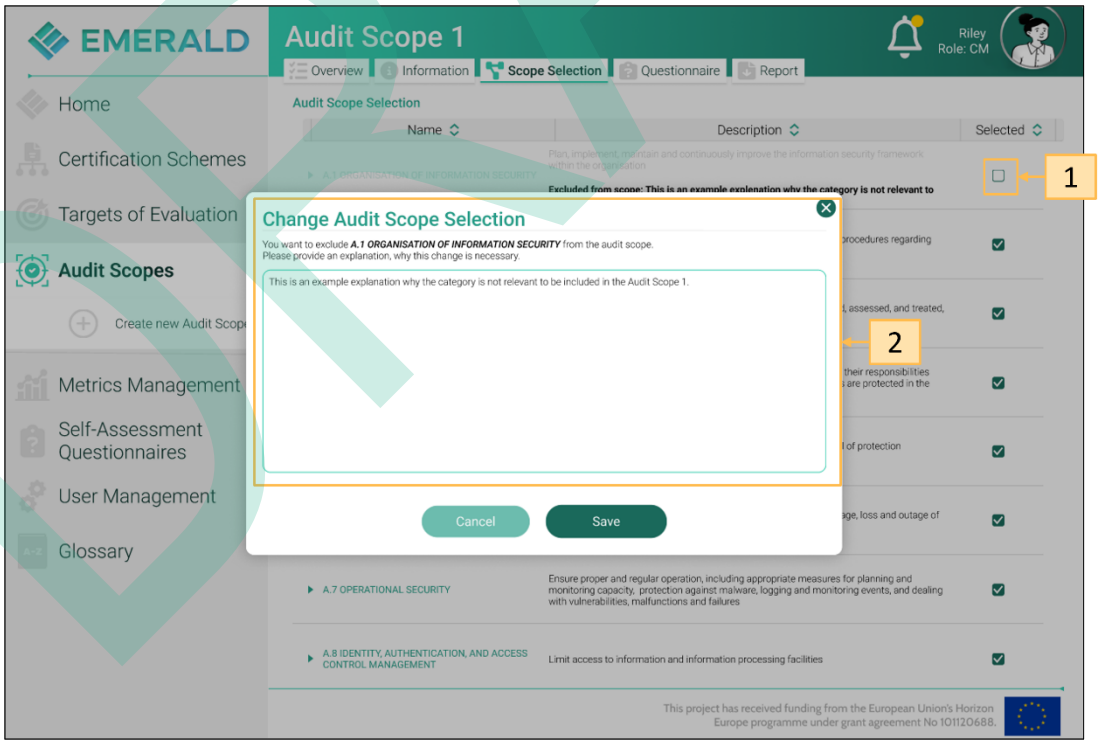

Figure 85. Audit Scope – Scope Selection Tab – Deselect Category

It is also possible to click on an individual control and see which metrics have been assigned to the control (see Figure 86). On the one hand, the user gets a description about the control (see Figure 86, point 1). On the other hand, the user sees the metrics assigned to the control (see Figure 86, point 2). For each individual metric, the user can change its applicability. If a user decides to deselect a metric, then the user has to add an explanation why this metric is not applicable anymore (this looks similar to Figure 85, point 2). Additionally, when clicking on the "Add new" button (see Figure 86, point 3), the user also has the possibility to add another metric from the set of available metrics (see Figure 86, point 4) and save it accordingly (see Figure 86, point 3).

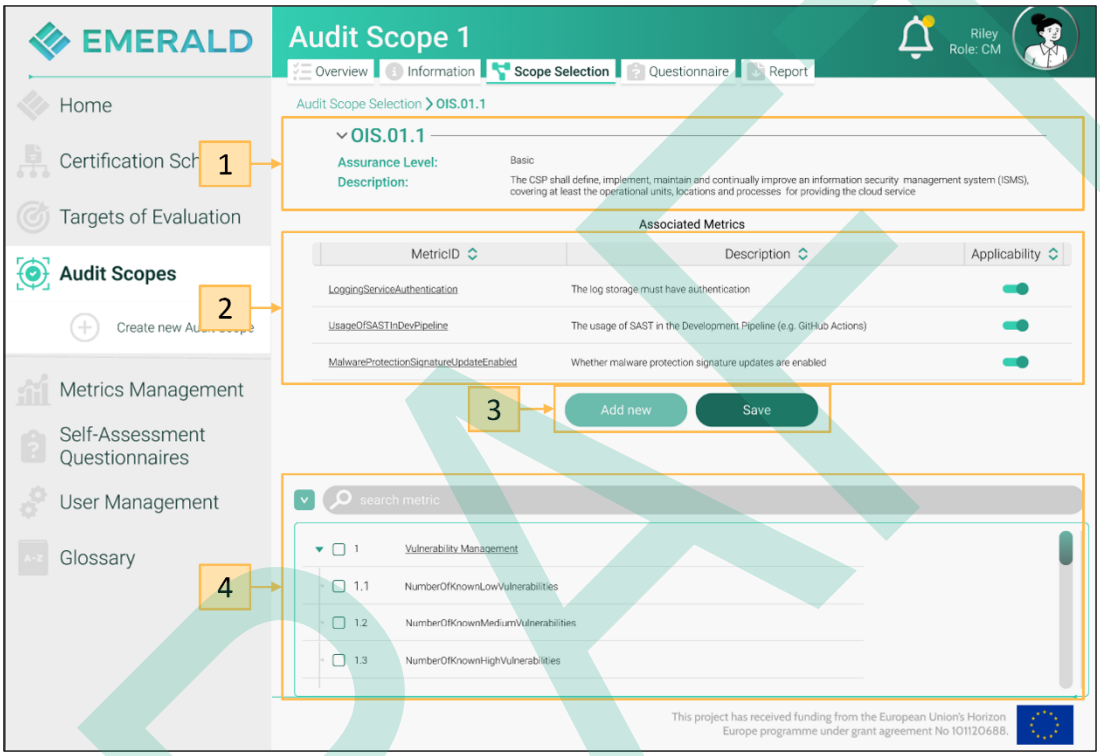

Figure 86. Audit Scope – Scope Selection Tab – Control and Metrics

4.5.3.3 Questionnaire Tab

The self-assessment questionnaire tab is only available if the certification scheme selected for the audit scope is EUCS. Otherwise, this tab is not visible in the audit scope.

When a user clicks on the questionnaire tab for the first time, the user can create a new questionnaire as shown in Figure 87, point 1.

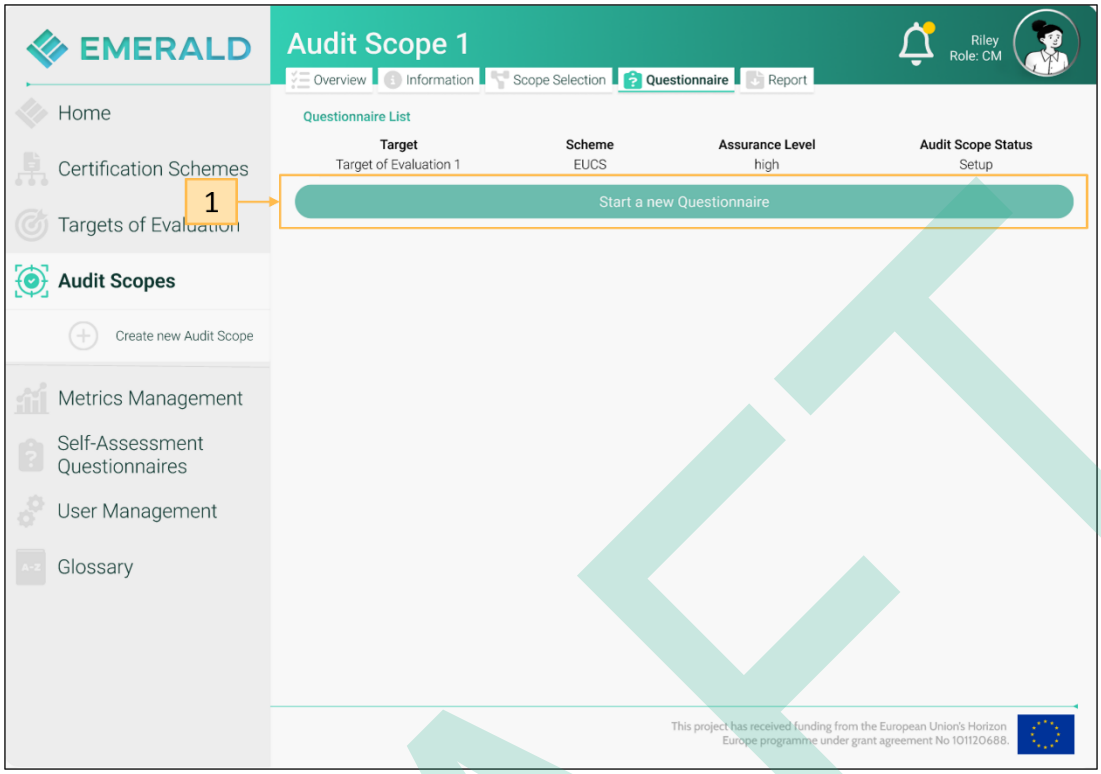

Figure 87. Audit Scope – Questionnaire Tab – New Questionnaire

If there has already been created one or more questionnaires for the audit scope, the user gets shown a list of the available questionnaires as shown in Figure 88. For each questionnaire, a user sees the creation date, when it was updated for last time, and by whom. Additionally, a user (depending on the user rights) can access the history of the questionnaire and delete it.

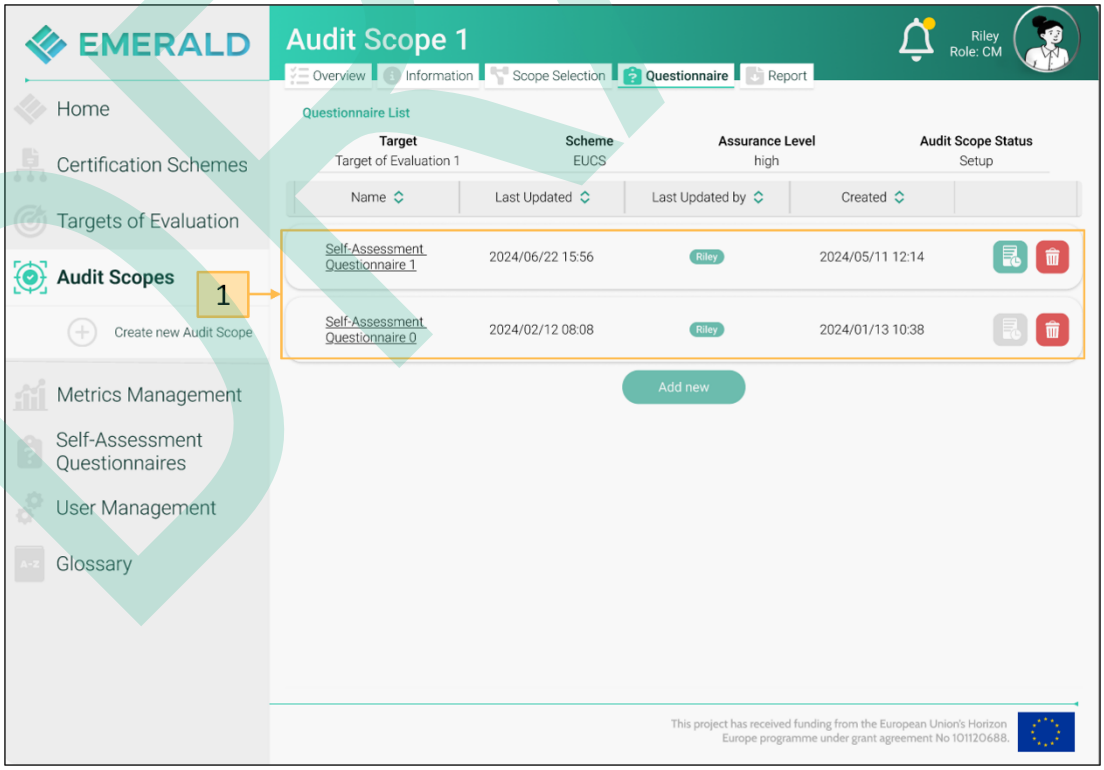

Figure 88. Audit Scope – Questionnaire Tab – Existing Questionnaires

After entering a questionnaire, a user is shown a doughnut diagram Figure 89, point 1 about the self-assessment control compliance status of the questionnaire. A control question can be not answered (white), compliant (green), partially compliant, non-compliant (red), or not applicable (grey). Thus, this diagram shows to what extent the questionnaire has already been filled in. Figure 89, point 3 offers the possibility to download the questionnaire. When clicking on the green segment of the doughnut diagram, more information about the compliant controls is provided, as depicted in Figure 90.

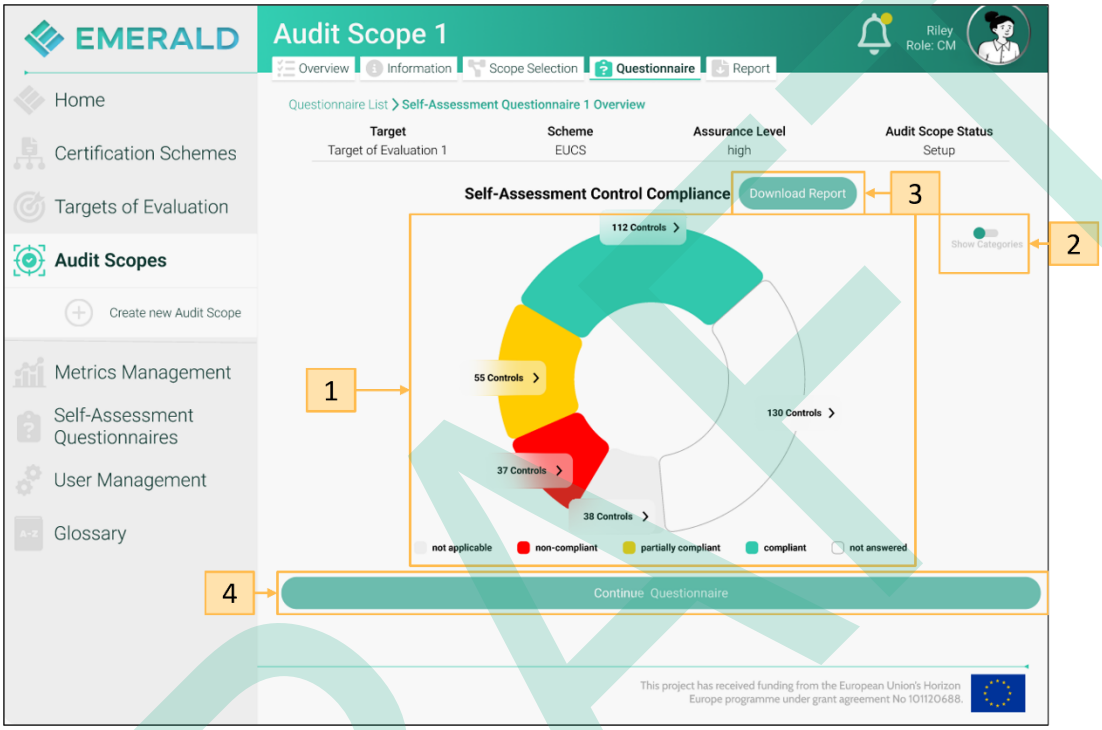

Figure 89. Audit Scope – Questionnaire Tab – Doughnut Diagram

Figure 90, point 1 shows that the green part (compliant controls) of the chart is highlighted and present in Figure 90, point 2, the list with all compliant controls. If a user clicks on the other coloured parts of the doughnut diagram, the respective controls in the respective status are listed.

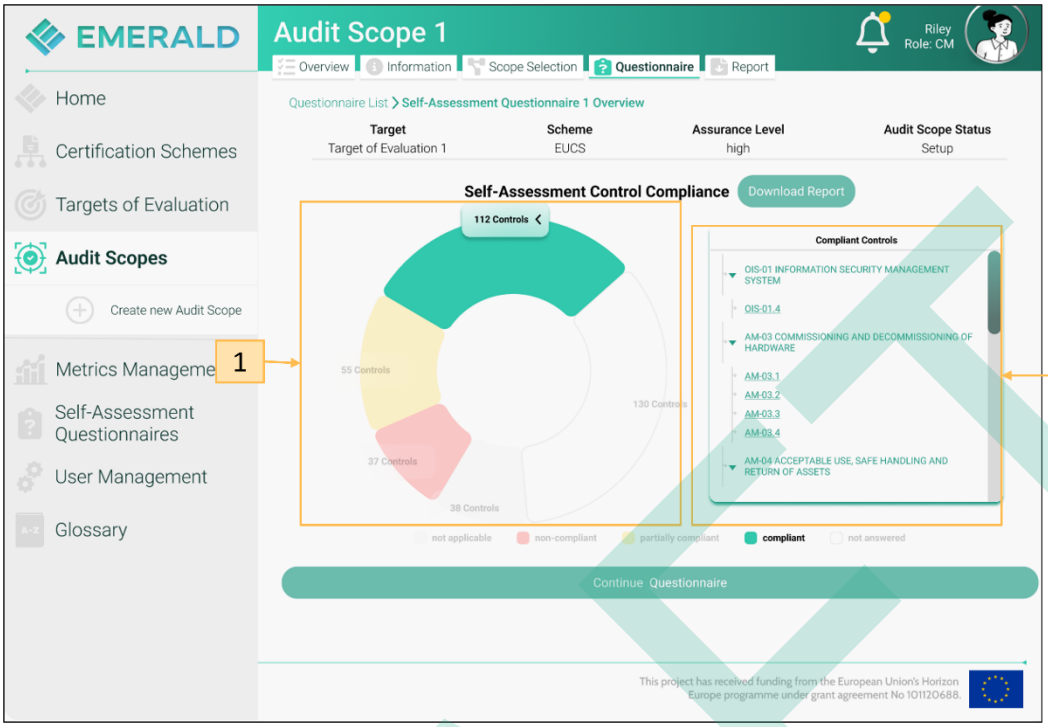

Figure 90. Audit Scope – Questionnaire Tab – Compliant Controls

When clicking on Figure 89, point 2, the view is changed to a bar chart visualisation as shown in Figure 91. For each category of the EUCS, a bar chart shows the compliance status of the controls in the questionnaire (Figure 91, point 1). Clicking on Figure 91, point 2 redirects the user back to the doughnut view (Figure 89).

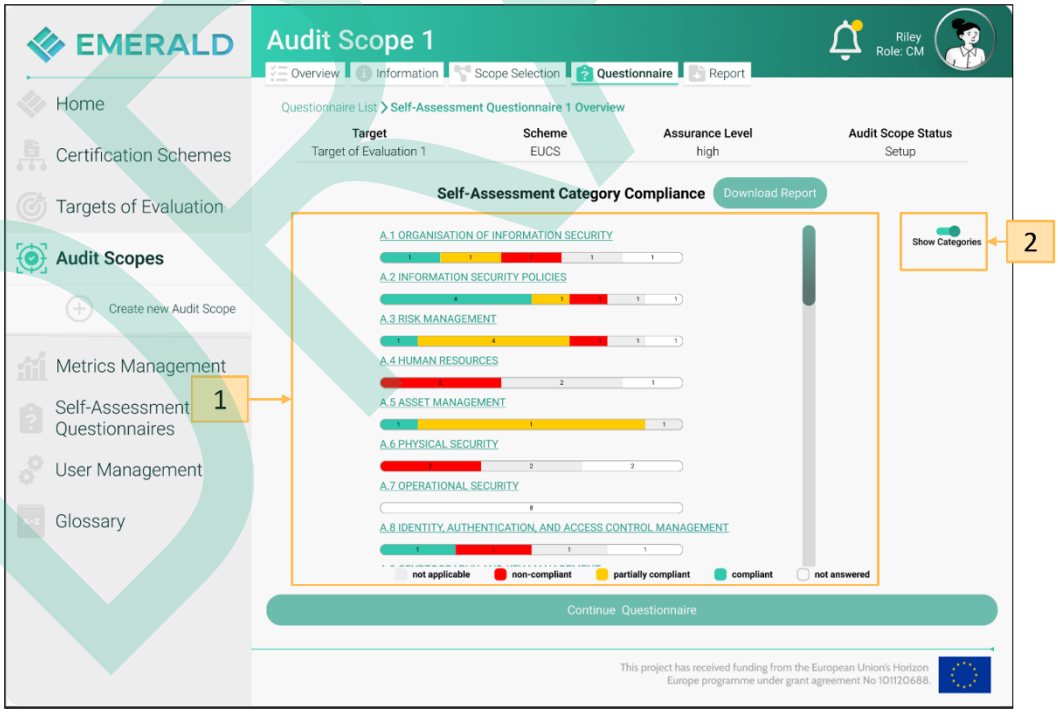

Figure 91. Audit Scope – Questionnaire Tab – Bar Charts

Figure 89, point 4 “Continue Questionnaire” leads the user to the questions of questionnaire.

Figure 92 and Figure 93 show an example of the questions. Figure 92, point 1, provides an overview of the progress of the questions answered so far. Figure 92, point 2, provides an overview of the progress of the answered questions for a category – in this case, category "A.1 Organisation of Information Security". Figure 92, point 3, shows the status of the individual control being answered. For example, OIS-01.1 has not been answered; OIS-01.2 is not applicable; OIS-01.3 is partially compliant; OIS-01.4 is compliant, and OIS-01.5 is not compliant. Figure 92, point 3 shows that the control OIS-01.1 is currently active. Therefore, Figure 92, point 4 presents the description about the related sub-ordinate category OIS-01 and the description of the control OIS-01.1 itself. Below (Figure 92, point 5) a user can find the different questions related to the control. For each of the question a user can set the status to fully supported, partially supported, not supported at all, and not applicable. Additionally, a user can upload or describe the evidence and an add a comment.

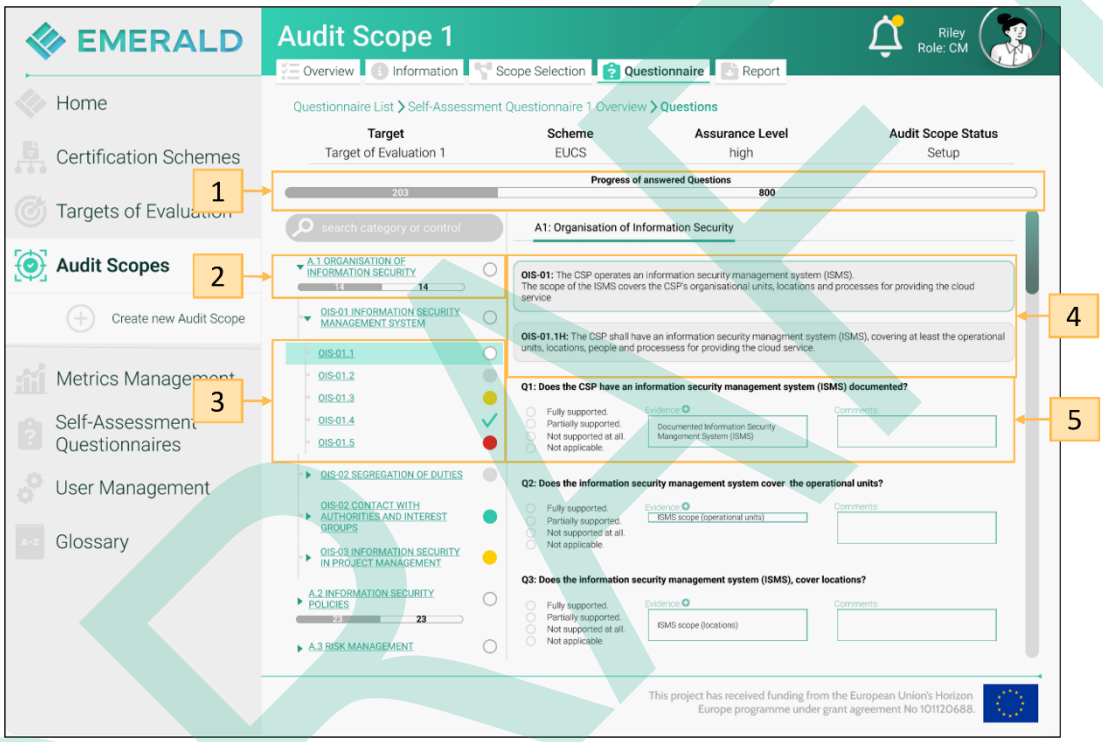

Figure 92. Audit Scope – Questionnaire Tab – Questions 1

At the end of a questionnaire page (see Figure 93), auditors can add some information (see Figure 93, point 1) such as mentioning non-conformities of the control. The compliance status of the control is automatically calculated (see Figure 93, point 2) depending on the answers given. The calculation of the compliance status is presented in Table 12.

Table 12. Audit Scope –Tab Questionnaire – Calculating the Compliance Status

Answer to questions	Compliance Status
All answers are „fully supported" or "not applicable	Compliant
All answers are "not supported at all" or "not applicable"	Non-Compliant
All answers are "not applicable"	Not applicable
Any answer is "not supported at all"	Partially compliant
Any answer is "partially supported"	Partially compliant

Figure 93, point 3 offers the possibility to got to the previous or the next page or to leave the questionnaire.

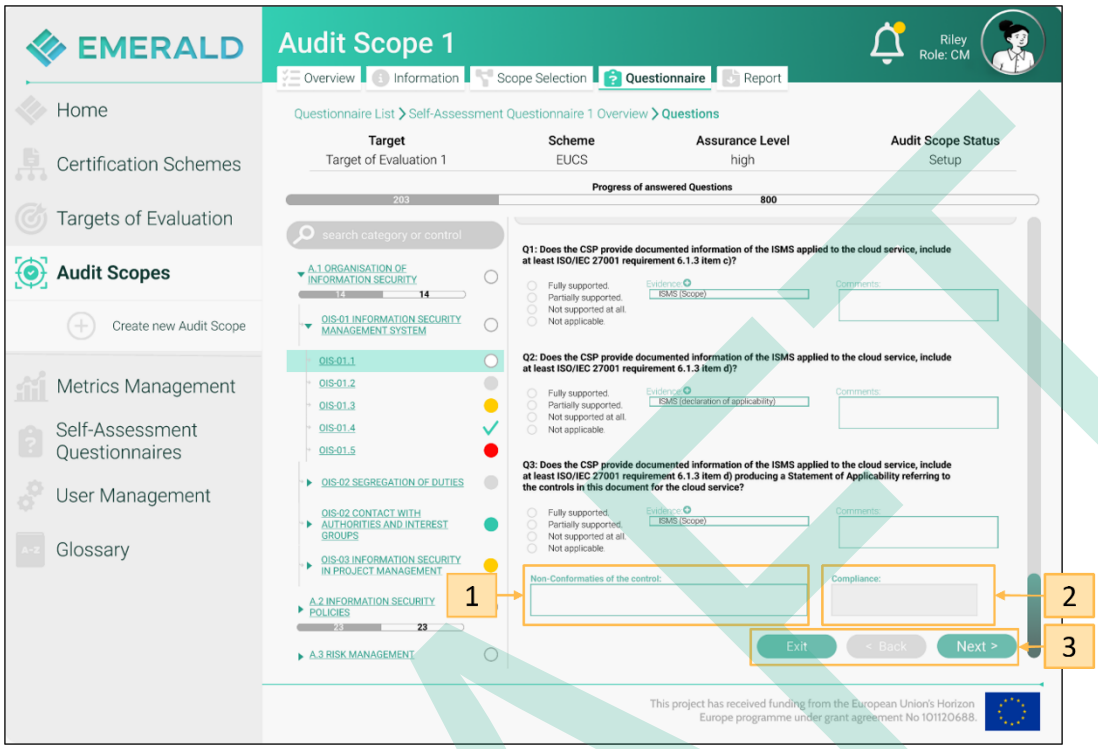

Figure 93. Audit Scope – Questionnaire Tab – Questions 2

4.5.3.4 Report Tab

The reports available for an audit scope can be accessed when clicking in Figure 68, point 1 on the report tab. The report functionality is divided into two views. The "Audit Report History" and the "Track Record of Evidence". Figure 94 presents the Audit Report History. For switching between the two views, a user can use the two tabs (see Figure 94, point 1). Audit Report History presents the evolvement of the compliance status of the controls over time in a diagram (see Figure 94, point 2). Below, monthly reports can be downloaded. For example, Figure 94, point 3 presents the monthly report for June 2025. When clicking on the Download Report button, this report is downloaded as a PDF document. When clicking on the Create Snapshot button (see Figure 94, point 4), a report of the current status of the audit scope is created and downloaded.

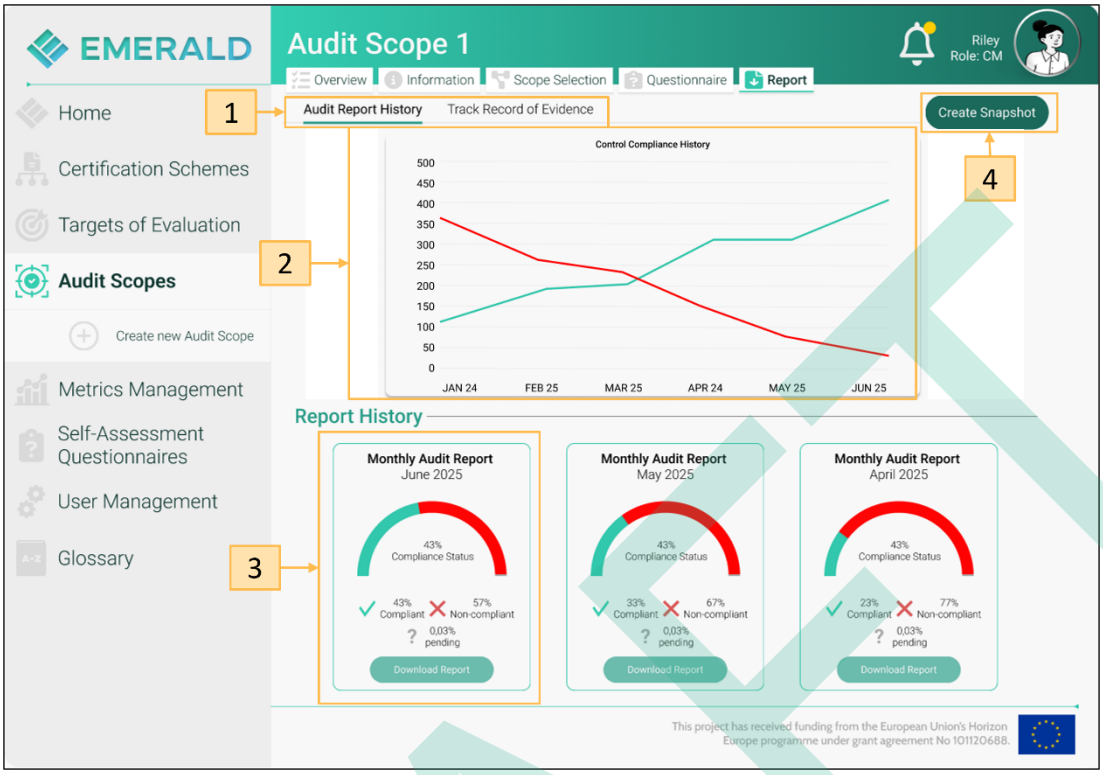

Figure 94. Audit Scope – Report - Audit Report History

Figure 95 presents the Track Record of Evidence. In this view a user first gets an overview of the compliance status of the current audit scope (Figure 95, point 1 and point 2). Then, the user can select which category should be shown (Figure 95, point 3). The information presented (Figure 95, point 4) shows first the "Compliance Proof" part - compliance information for each control.

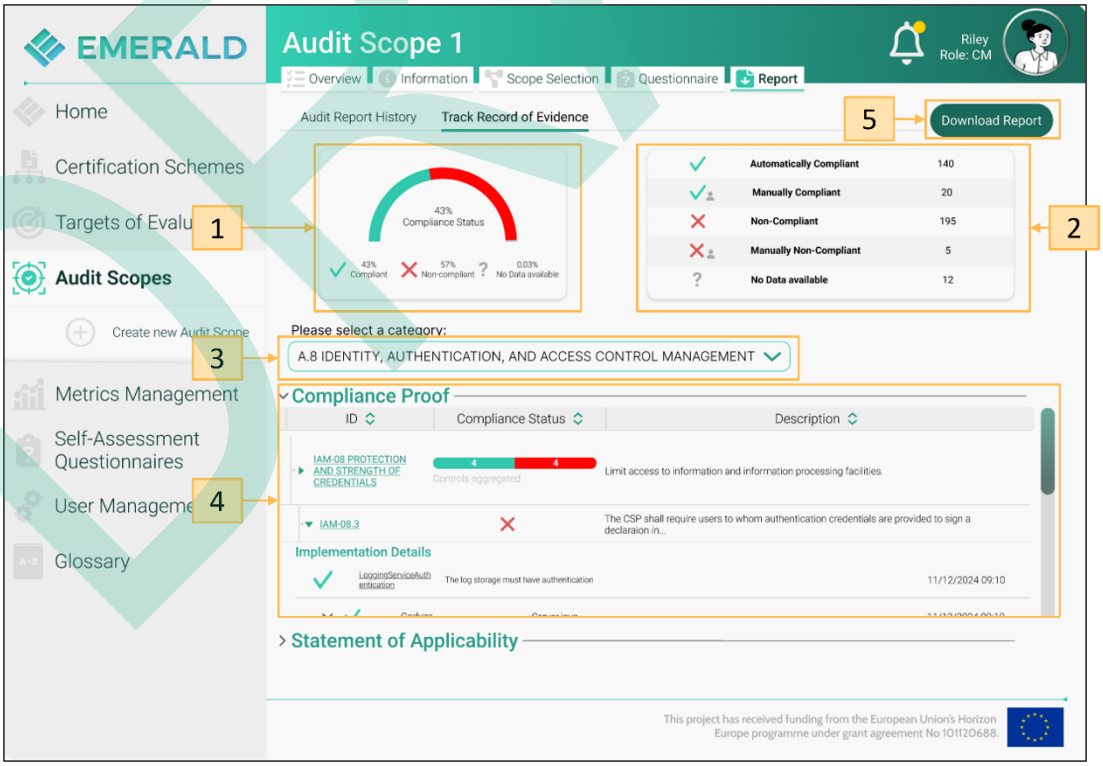

Figure 95. Audit Scope – Report – Track Record of Evidence – Compliance Proof

When scrolling down in the list (Figure 95, point 4), the “Statement of Applicability” is presented as shown in Figure 96, point 1.

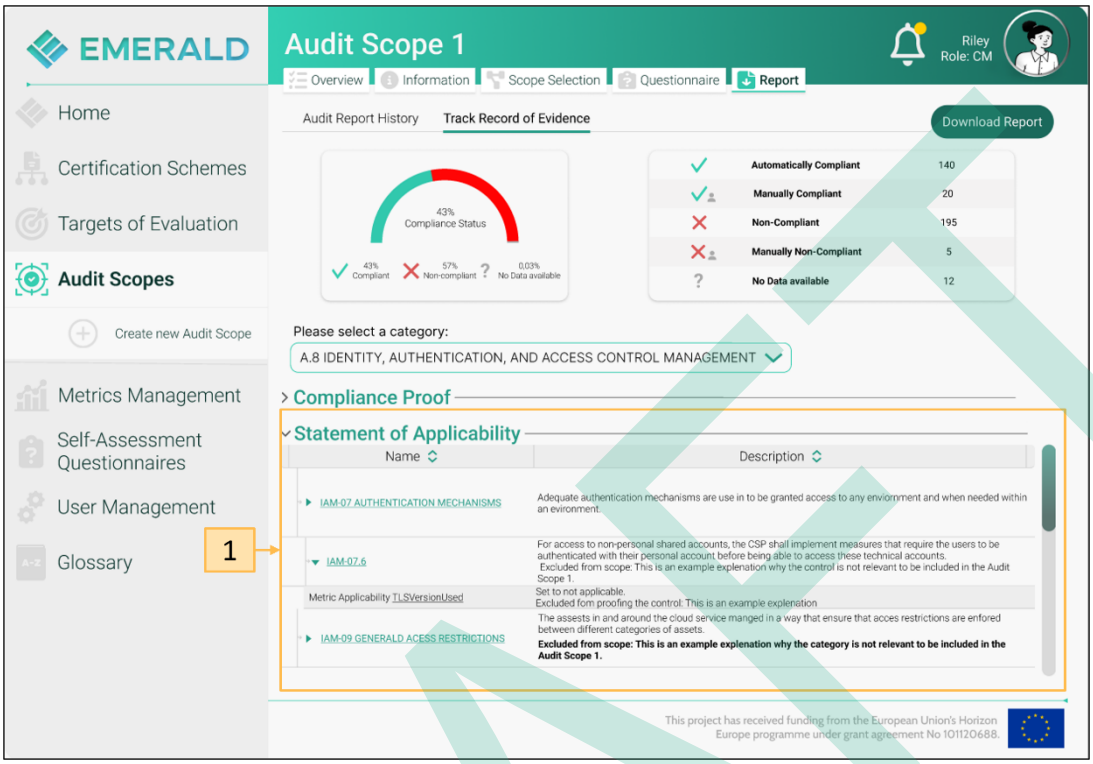

Figure 96. Audit Scope – Report – Track Record of Evidence – Statement of Applicability

The “Download Report” button, as presented in Figure 95, point 5, offers the possibility to download a report. A user has the possibility to decide which content should be included in the report (see Figure 97, point 1) and in which format the report should be downloaded (see Figure 97, point 2).

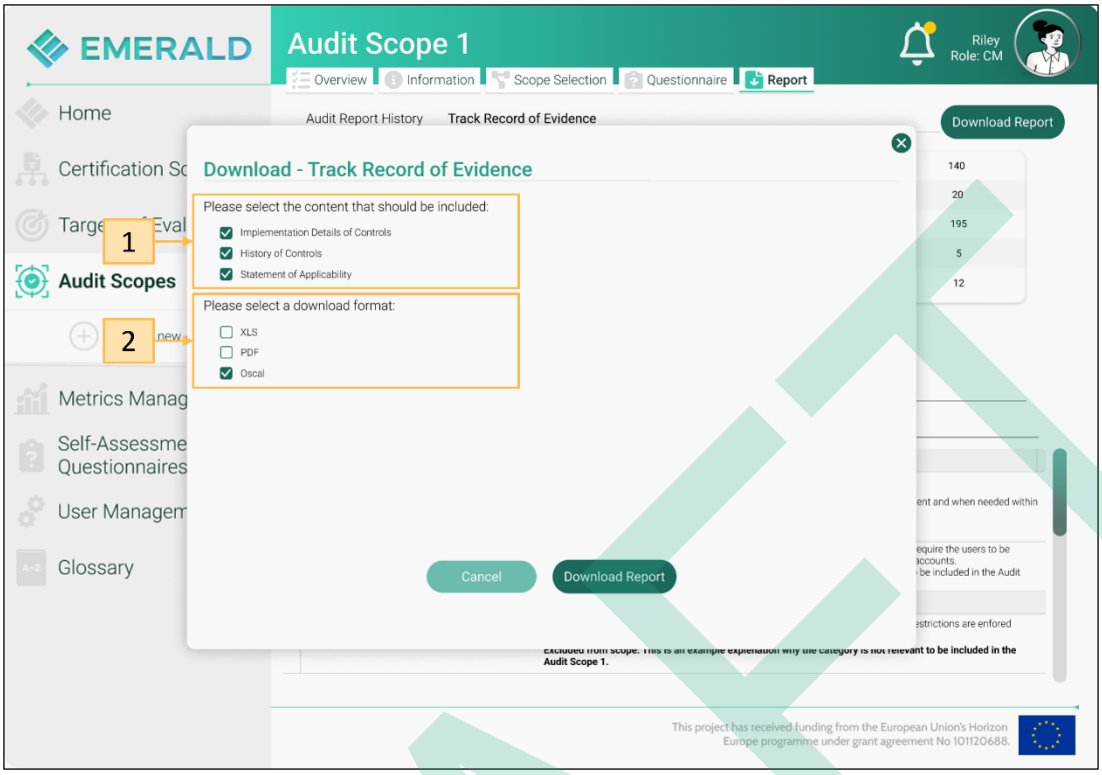

Figure 97. Audit Scope – Report – Track Record of Evidence – Download Report

4.6 Metrics Management

The metrics management view can be entered when clicking on Figure 21, point 5. The Metrics Management section allows viewing the categories, the assigned metrics assigned to the categories, and in which audit scopes the individual metrics are used. Figure 98 presents the overview of the metrics management. First, it presents an overview of the existing categories like for example, Figure 98, point 1. When clicking on a category, all metrics assigned to this category are listed (Figure 98, point 2). Clicking on the "Synch Repository" button (Figure 98, point 3) will synchronize the metrics with the metrics management repository (e.g. import new metrics).

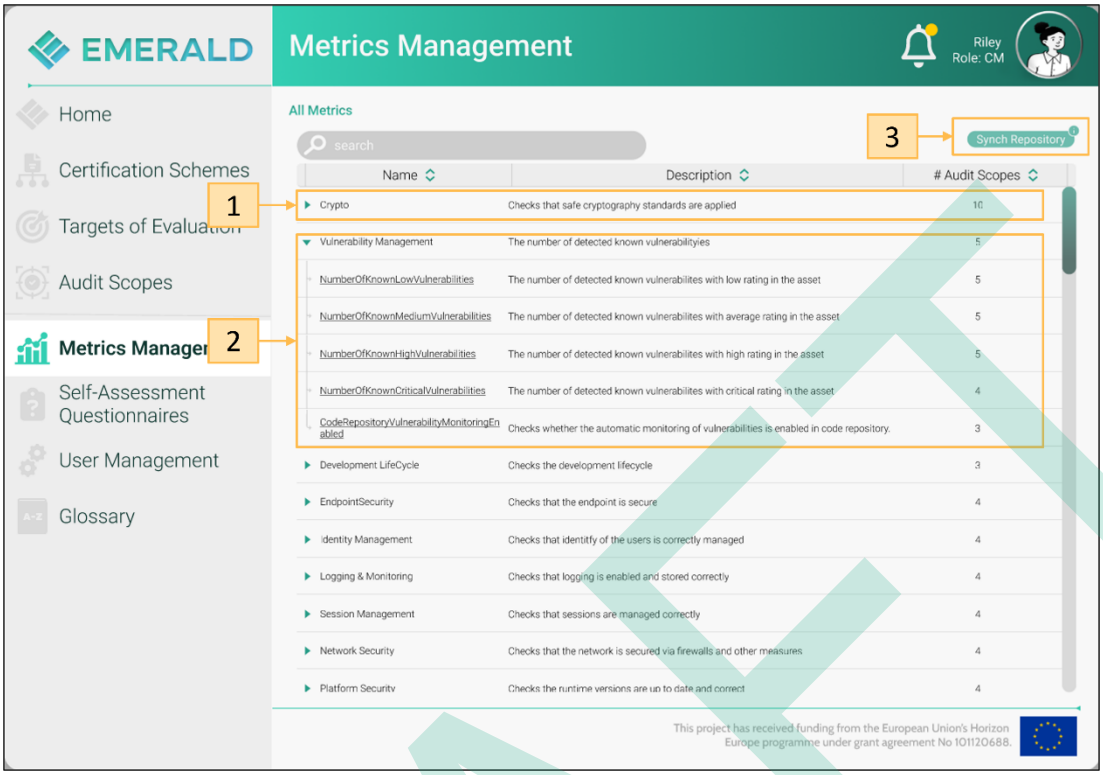

Figure 98. Metrics Management - Overview

When clicking on a metric, for example "TLSVersionUsed"– see Figure 99, point 1 – the view presents in which audit scopes the metric is used. The metric selected is used in Audit Scope 1, and the related controls that the metric is assigned to are shown (see Figure 99, point 3).

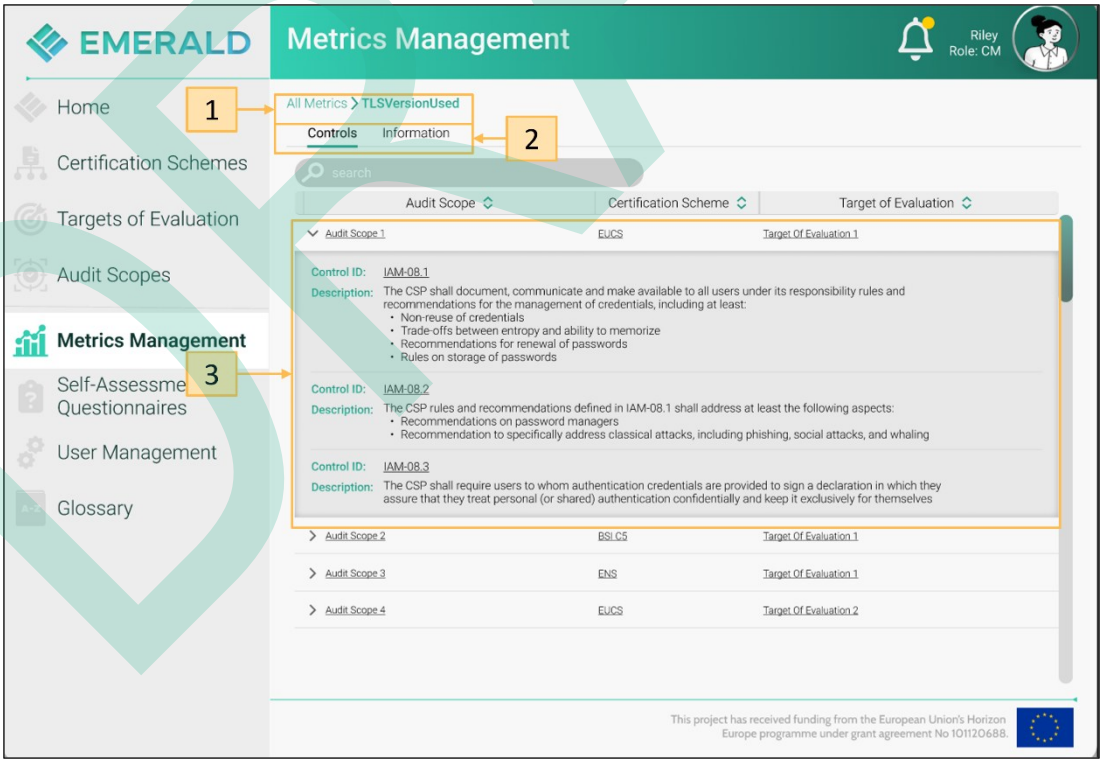

Figure 99. Metrics Management – Metrics in Audit Scopes

When clicking on Information on Figure 99, point 2, more information about the metric is presented, as shown in Figure 100, point 2.

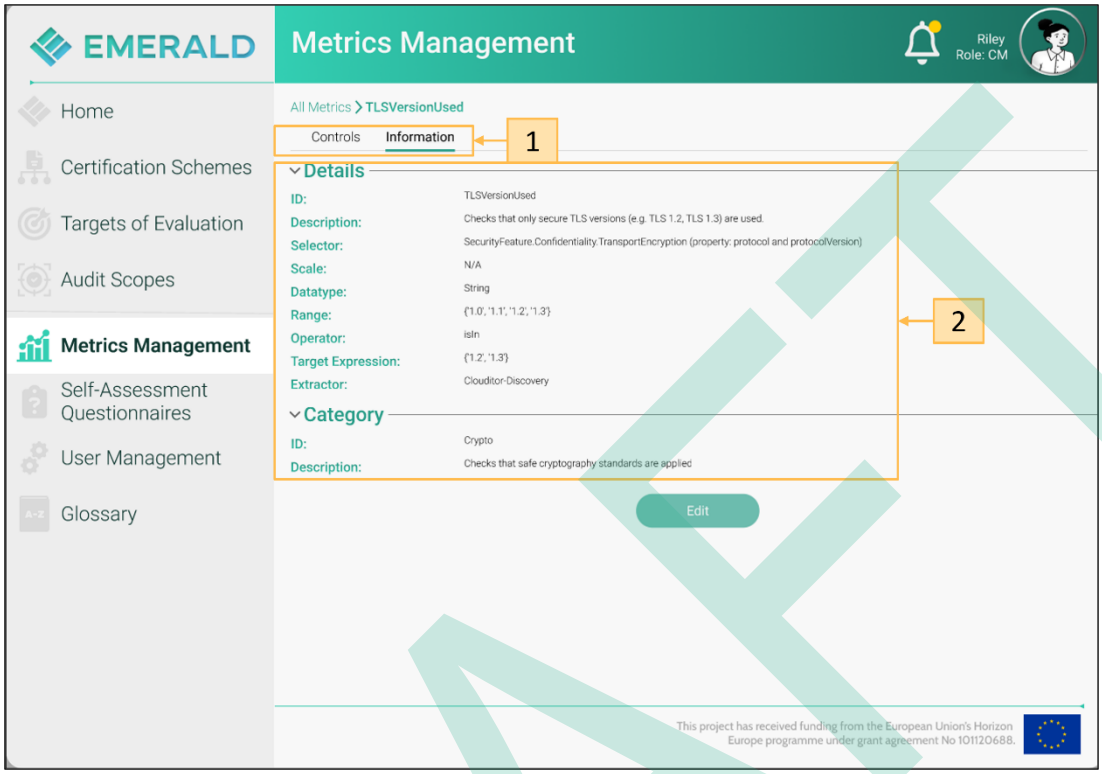

Figure 100. Metrics Management - Metrics Information

It is important to note that only specific fields of a metric can be edited directly within the EMERALD UI. To modify any other fields, or to add a new metric, users must make these changes directly in the Metrics Repository.

4.7 Self-Assessment Questionnaires

The self-assessment questionnaires are accessible in the related audit scope but can be also accessed in the Self-assessment Questionnaire section when clicking in Figure 21, point 6. Figure 101 presents the overview of the available self-assessment questionnaires per audit scope (depending on the user rights). For example, Figure 101, point 1 shows that two self-assessment questionnaires are available for audit scope 1 and one self-assessment questionnaire is available for audit scope 4. For each questionnaire, the following information is presented: the related audit scope, target of evaluation, the assurance level of the EUCS, when the questionnaire was lastly updated, and the creation date of the questionnaire. When clicking on the name of a questionnaire, the questionnaire is opened as shown in Figure 89.

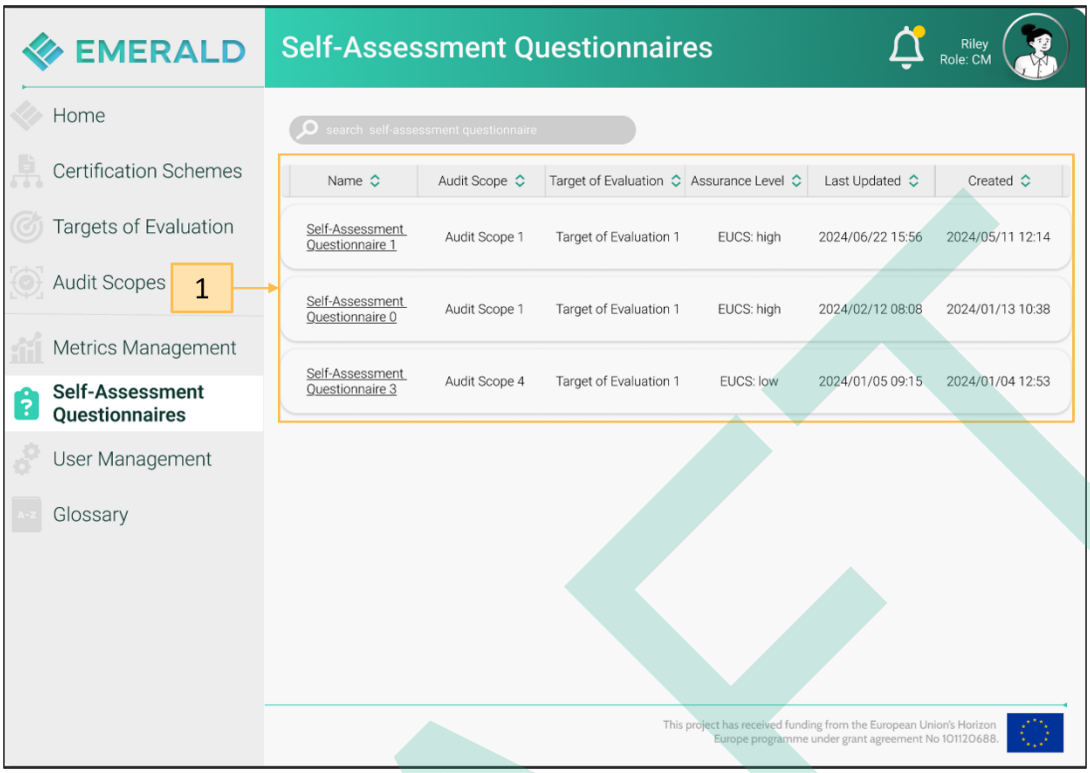

Figure 101. Self-Assessment Questionnaire

4.8 User Management: Roles and Access Rights

The user management allows to manage the EMERALD users. Users themselves cannot be created through the EMERALD UI, instead they have to be created in keycloak[6] – an Open-Source Identity and Access Management software used for the EMERALD CaaS framework.

Figure 21, point 7 allows a user to enter the user management. Figure 102 shows the entry page of the user management. In this view, all EMERALD users are shown like for example Figure 102, point 1 or point 2. When clicking Figure 102, point 3 a new user – who has already been created in keycloak can be invited to the EMERALD UI.

[6] https://www.keycloak.org/

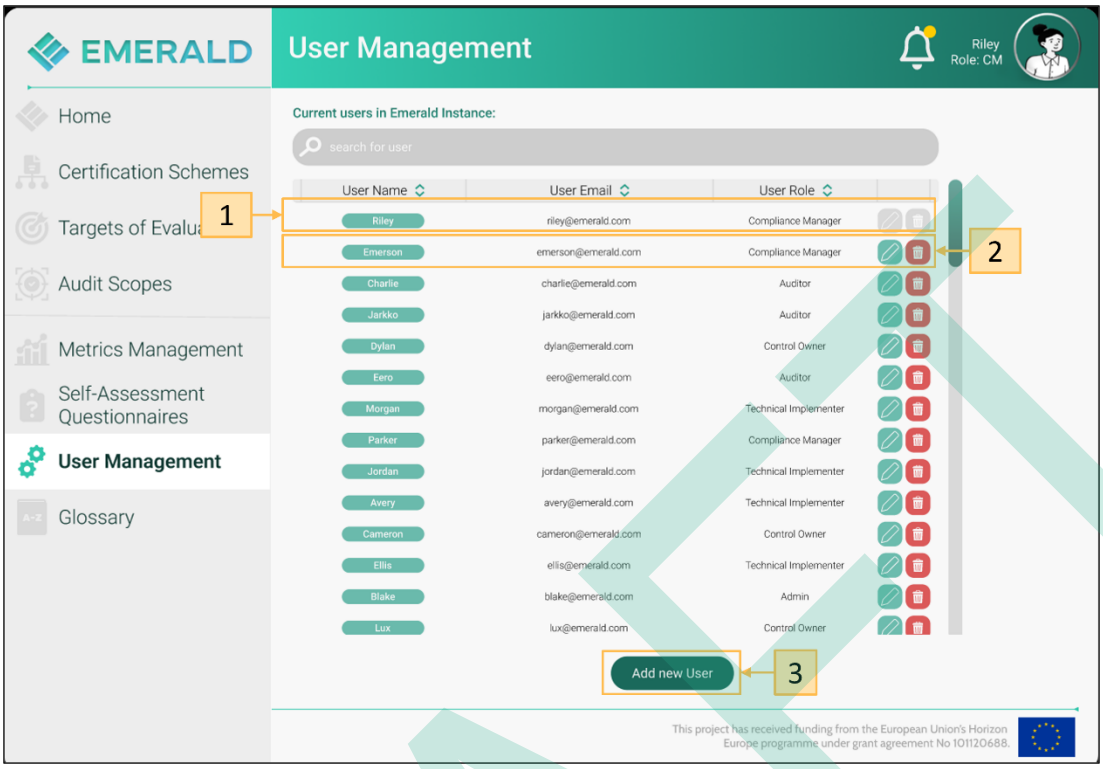

Figure 102. User Management – Overview

To add a new user, the email address or the user ID needs to be entered (see Figure 103, point 1) and the corresponding role needs to be selected (see Figure 103, point 2). When clicking on Figure 103, point 3 an invite is sent to the user, and after accepting this invitation the user is able to access the EMERALD UI.

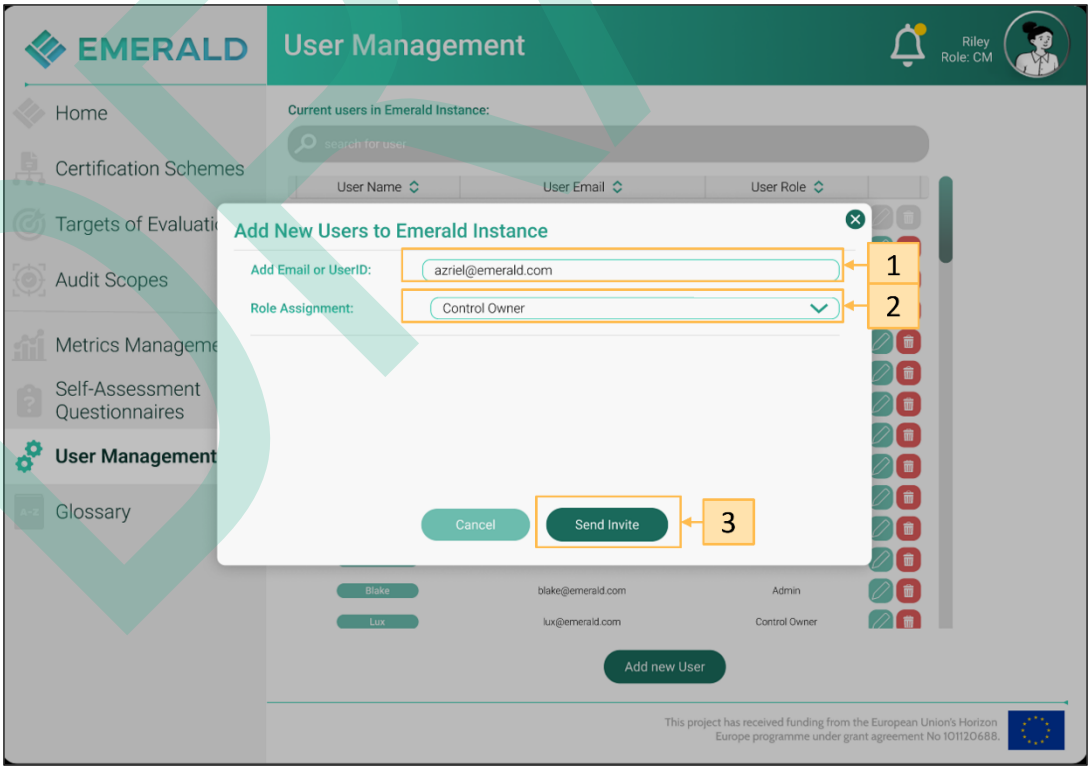

Figure 103. User Management – Add new User

Additionally, it is also possible to edit or delete an existing user (Figure 102, point 2 – right buttons). Figure 104, point 1 a new username can be entered and Figure 104, point 2 allows to change the role of the user.

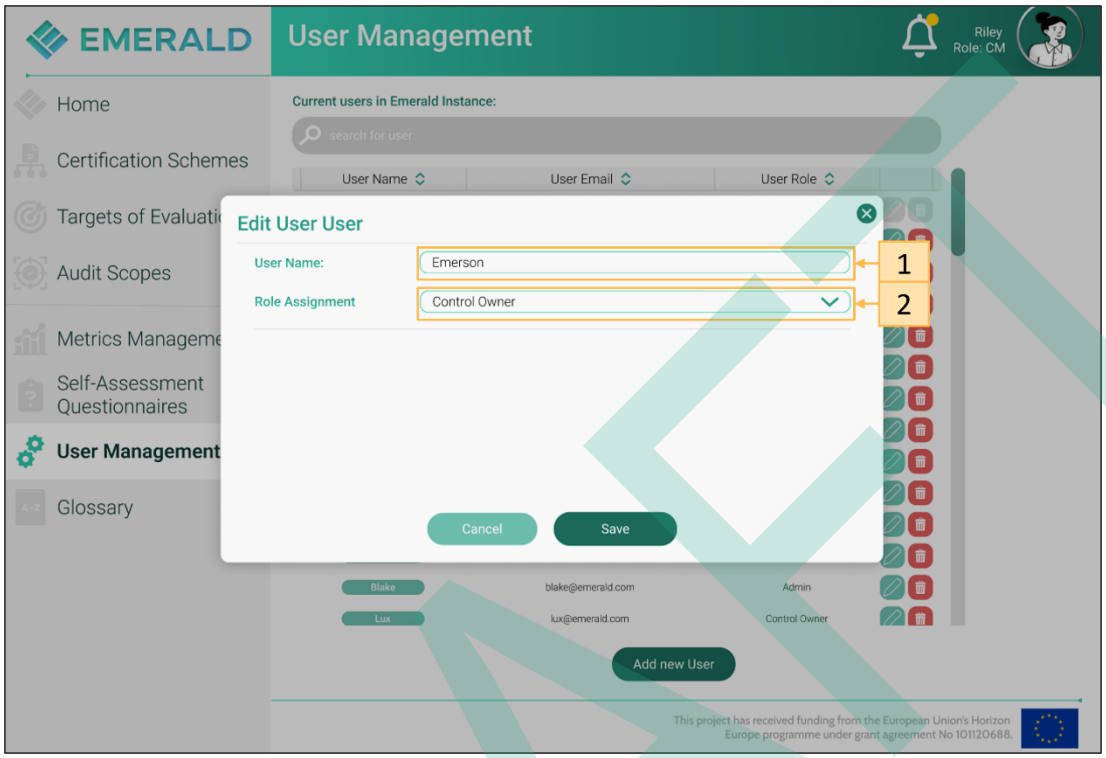

Figure 104. User Management – Edit User

4.9 Glossary

The EMERALD glossary can be accessed when clicking in Figure 21, point 8. The glossary provides a definition of the terms used in the context of EMERALD. These definitions are gathered as part of WP1, Task 1.2 Architecture.

Figure 105 presents the glossary in the EMERALD UI. There is a list of terms used, and when clicking on the term, the description is presented, like for example in Figure 105, point 1 or point 2.

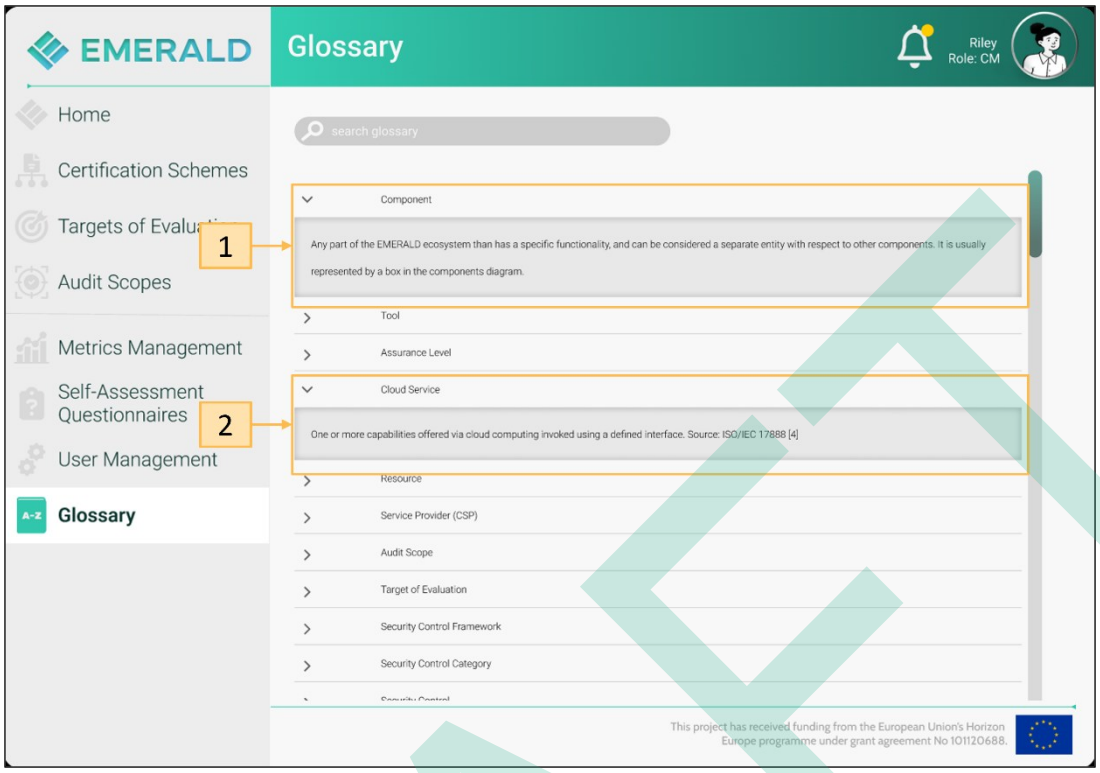

Figure 105. Glossary – Glossary Entry

5 Validation

5.1 Insights from the Target Users

At the general assembly in Pisa (March 2025), we conducted a validation round with all consortium partners to get further feedback regarding the implemented EMERALD UI features in the clickable mock-up.

5.1.1 Methodology

Procedure:

At the beginning of the 2-hour workshop, we presented the consortium partners what we expect them to do in the workshop. First, we divided them into groups of three people, where each group member was from a different consortium partner. Each group received printed instructions on what to do. Second, we asked them to fill in a general questionnaire. Afterwards, we asked them to access the clickable EMERALD mock-ups and go step-by-step through the three prepared user journeys. After each user journey, they were asked to provide feedback through the feedback questionnaire.

Evaluation Tools and Materials:

- General Questionnaire: This questionnaire consisted of a consent form including a neutral participant ID, so that all participants confirmed that we are allowed to use collected data for the project and for a publication. This was followed by a demographic questionnaire.
- User Journeys: Altogether we have used nine different user journeys, which were based on the available functionality of the clickable mock-up. It is important to remark that each group received three different user journeys related to three different EMERALD personas. We also divided the user journeys according to their length (some user journeys had more steps and took longer than others), so that the time spent going through all three user journeys was similar across all groups.
- Feedback for each user journey: This questionnaire consisted again of a consent form and the unique participant ID. Then we had a set of items to ask about the user journey and its implementation in the UI. We used the ”System Usability Scale” (SUS, [21]) to evaluate the participants perceived usability of the clickable mock-up. The System Usability Scale (SUS) is a widely used and reliable tool for assessing system usability. It consists of ten Likert-scale items. Each item is rated on a five-point scale ranging from *“Strongly disagree”* to *“Strongly agree.”* Responses are converted into an overall usability score from 0 to 100, with higher scores indicating greater perceived usability. At the end of each questionnaire per user journey we requested for additional comments and feedback.

Participants:

A total of 25 participants from the EMERALD consortium participated in the study. Among the participants, 13 identified as male, 11 as female, and one preferred not to disclose their gender, with a mean age of $M = 39.96$ ($SD = 10.6$). Seven of them have a PhD degree or higher, 16 have a MSc or equivalent, one has a short-cycle Tertiary Education (e.g., apprenticeship) and one BSc or equivalent. Seventeen of them work in Information Technology (IT), six in science and research, and two in economy & finance with an average work duration of $M = 14.0$ ($SD = 9.3$) years. Regarding their experience in UI/UX design, 14 stated to have little experience, three have basic experience, and five perceived themselves as UIUX expert.

5.1.2 Results

Altogether, nine different user journeys have been used in the validation round.

Table 13 shows how often each user journeys was conducted by the different groups.

Table 13. Number of how often each User Journey was conducted.

User Journeys	Number of times worked through
MORGAN – Checking Metrics and Evidence	9
CHARLIE – Preparation for an audit by an internal auditor	7
DYLAN – Control Implementation	6
EMERSON – Bring your own certification scheme (BYOCS)	6
RILEY – Manage all Controls of an Audit Scope	5
RILEY – Managing a New Audit Scope	5
RILEY – Accompanying an Audit	5
JARKKO – Scoping	5
JARKKO – Preparing for Audit	4

For each user journey, we asked how easy it was to complete the user journey using the EMERALD UI on a 5-point Likert scale (very easy (5) – very difficult (1)). The users rated the completion of the user journey as very easy to easy with 61,5%, as neither easy nor difficult with 28,9% and only 9,6% rated it as difficult to very difficult. We also asked users how confident they were that they had completed the user journeys correctly. Nearly half of the participants (48,1%) reported being very confident. Fifteen percent (15,4%) of the responses were distributed equally across the categories of confident, neither confident nor unconfident, and not confident. Only 5,7% of participants reported being not very confident in having correctly completed the user journeys. To evaluate the subjectively perceived usability of the clickable mock-up, we used the System Usability Scale (SUS, [21]). The SUS scores varied across the different user journeys, ranging from 68.50 for Riley – Manage all Controls of an Audit Scope to 42.50 for Jarkko – Scoping. A detailed overview of the SUS scores per user journey is provided in Table 14.

Table 14. System Usability Scores for each User Journey.

User Journeys	System Usability Scale (SUS) Score
RILEY – Manage all Controls of an Audit Scope	68.50
RILEY – Managing a New Audit Scope	67.50
DYLAN – Control Implementation	61.67
EMERSON – Bring your own certification scheme (BYOCS)	57.50
CHARLIE – Preparation of an audit by an internal auditor	55.36
MORGAN – Checking Metrics and Evidence	53.89
JARKKO – Preparing for Audit	53.13
RILEY – Accompanying an Audit	50.50
JARKKO – Scoping	42.50

The overall SUS results indicate an average score of 56.63 (SD = 13.21). According to Bangor et al. [22], this value falls between the categories “OK” and “Good.” Considering that the evaluation

was based on a clickable mock-ups rather than on a fully implemented user interface, this result is very encouraging.

The variation in SUS scores across user journeys can be partly explained by insights from the open-ended feedback. Several participants expressed frustration when attempting to interact with interface elements, such as buttons, that were not yet clickable. This limitation is inherent to the prototype, as not every possible interaction was implemented. Additionally, some users noticed that data entered or modified on one screen was not carried over to subsequent screens. This behaviour was also due to the constraints of the clickable mock-ups rather than the intended functionality of the final product.

Further analysis of the qualitative feedback revealed several recurring usability themes. Overall, participants expressed positive impressions of the interface and its learnability. As one participant noted, *"We use audit scope in different journeys, and during the second time it is easy to go through, so it is fast to learn how to use it."* Another stated, *"It was a nice experience given that it was the first time I was using this interface"*. These comments suggest that the initial onboarding experience was perceived as intuitive and that the interface supports a relatively quick learning curve.

Despite these positive impressions, several usability challenges were identified. Some participants encountered prototype-related limitations, reporting issues such as *"non-clickable buttons, data not carrying over between screens, [and] incomplete functionality"*. Others highlighted navigation challenges, for example: *"Unclear difference between buttons/icons, missing 'back' functionality, [and] difficulty navigating between metrics, controls, and assessments"*.

Beyond prototype-specific issues, participants experienced uncertainty when moving between controls, metrics, and assessment results. The visual design and information hierarchy were also perceived as inconsistent, with some screens appearing overcrowded while others lacked sufficient emphasis on key actions. Furthermore, users reported difficulties in understanding system states and notifications, indicating a need for clearer terminology, labelling, and visual cues. Finally, several participants expressed a desire for additional guidance, suggesting the inclusion of tooltips, contextual hints, and explanatory help pages, particularly when interacting with unfamiliar features.

Importantly, a significant portion of the negative feedback stemmed from the limitations of the clickable mock-ups used during testing. Missing interactions, non-functional buttons, and the absence of data persistence across screens frequently disrupted user flows. Other concerns, such as filtering inconsistencies and the scalability of controls management, highlighted areas that required refinement in the design.

These insights were incorporated into the subsequent design iteration, which introduced clearer visual hierarchies, improved status communication, and enhanced guidance mechanisms. As a result, many of the usability issues identified during testing have since been addressed, laying a stronger foundation for a more intuitive and user-friendly interface.

5.2 Insights from the EAB

On the 30th of September 2025 the 3rd External Advisory Board meeting (EAB) was held. In this meeting, we presented the co-creation and co-design approach applied (see Figure 1), then we shortly presented the overall EMERALD process before we conducted a short in-depth presentation of the clickable mock-ups. Altogether four external advisory board members, who are experts in the cybersecurity domain, participated in the meeting.

During meeting, the discussion focused on the articulation and standardisation of control safeguards in cybersecurity assessment and compliance. It was noted that the recent normative versions published by ETSI provide a valuable reference point for developing structured languages that can support automation and interoperability in tool implementation. Several members highlighted the relevance of EMERALD's ongoing work, particularly the development of notations for assessment results and controls, and the importance of aligning these efforts with related initiatives and standardisation bodies. The general need for better specification of controls and metrics in traditional audit preparation was emphasized, together with the ambition of EMERALD to contribute to a common and standardised language for cybersecurity risk assessment and compliance.

The discussion also addressed the perspective of end users, with pilot partners confirming the importance of practical and user-friendly mock-ups to ensure adoption in industrial contexts such as manufacturing. From a value proposition standpoint, the meeting raised questions regarding compliance status, interoperability with risk management tools, and connections with external initiatives such as the Cybersecurity Alliance (CSA). The Board noted that EMERALD's pilot work with CSA benchmarking approaches could provide useful insights, though further exploration of technical alignment with projects such as those led by TECNALIA and Fraunhofer was recommended.

No direct feedback was given on the co-creation and co-design approach or on the clickable mock-ups. However, one advisory board member underlined the value of using Figma, noting that it provides an efficient way to demonstrate the look and feel of the EMERALD solution to target users and to facilitate engagement with potential end users.

6 Conclusions

This deliverable presents the methodology applied in *Task 4.3 – Designing a User Interaction and User Experience Concept*, along with the final user journeys and clickable mock-ups developed within the EMERALD project.

Specifically, it includes:

- The **final set of user journeys** designed for the different personas, which served as the foundation for developing the clickable mock-ups.
- The **final version of the clickable mock-ups**, which act as the baseline for the implementation of the EMERALD UI.
- The **first validation results from target users**, confirming that the implemented mock-ups meet user needs.
- A summary of input from the External Advisory Board (EAB), which mainly addressed technical aspects rather than the direct design of the EMERALD UI.

This document constitutes the final version of the UI/UX results of Task 4.3, focusing on the design of the EMERALD user interaction and user experience concept.

7 References

[1] EMERALD Consortium, "D4.3 – User interaction and user experience concept – v1," 2024.

[2] EMERALD Consortium, "EMERALD - Annex 1 - Description of Action - GA 101120688," 2022.

[3] MEDINA Consortium, "CORDIS - EU research results," 2023. [Online]. Available: https://cordis.europa.eu/project/id/952633. [Accessed 10 2025].

[4] 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.

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

[6] 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.

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

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

[9] B. Westerlund, *Design Space Exploration: co-operative creation of proposals for desired interactions with future artefacts (Doctoral Dissertation),* 2009.

[10] C. Snyder, Paper prototyping: The fast and easy way to design and refine user interfaces, Morgan Kaufmann, 2003.

[11] C. Floyd, "A systematic look at prototyping," *Approaches to prototyping,* pp. 1-18, 1984.

[12] P. Ehn, *Work-oriented design of computer artifacts (Doctoral Dissertation),* Arbetslivscentrum, 1988.

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

[14] EMERALD Consortium, "D4.2 - Results of the UI-UX requirements analysis and the work processes - v2," 2025.

[15] B. Martin, B. Hanington and B. Hanington, 100 ways to research complex problems, develop innovative ideas, and design effective solutions, Rockport Publishers Beverly, 2012.

[16] C. Howard, User Journey Mapping: A Tool for Better User Experience., UX Design Institute., 2020.

[17] M. Stickdorn, M. E. Hormess, A. Lawrence and J. & Schneider, This Is Service Design Doing: Applying Service Design Thinking in the Real World., O'Reilly Media., 2018.

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

[19] D. Benedetto, C. Caimi, A. Ibrahim and Z. C. , *D5.4 - MEDINA integrated solution-v2,* 2023.

[20] EMERALD Consortium, "D1.4 EMERALD solution architecture-v2," 2025.

[21] J. Brooke, "SUS-A quick and dirty usability scale," *Usability evaluation in industry,* vol. 189(194), pp. 4-7, 1996.

[22] A. Bangor, P. Kortum and J. Miller , "Determining what individual SUS scores mean: Adding an adjective rating scale," *Journal of usability studies,* vol. 4(3), pp. 114-123., 2009.

8 APPENDIX A: Mock-ups derived from Interviews with Pilot Partners

In the context of WP4, we have conducted different types of interviews. On the one hand, we conducted an interactive interview session with all pilot partners at the general assembly in Bilbao (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. On the other hand, we conducted interviews with all pilot partners individually. The goal of these interviews was to elicit in-depth insights about the work of auditors (A), compliance managers (CM), and (chief information) security officers (CISO) in relation to continuous cloud auditing processes. From these, we were able to derive concrete work processes and 17 initial requirements (as presented in D4.2 [14]) for the development of the EMERALD UI/UX.

More information about the interactive interview session and the interviews conducted with the pilot partners was presented in D4.2 [14].

Based on the insights gained from the different types of interviews, as well as the derived UI/UX requirements, we derived a first set of paper-based mock-ups. These mock-ups were drawn with PowerPoint to get a first impression of how the EMERALD UI/UX could look like and which functionalities should be available.

Altogether, we were able to create around 20 mock-ups consisting of the following parts:

- **EMERALD Look & Feel:** Before starting with the development of the mock-ups, we developed an initial EMERALD Design, as depicted in Figure 106, which was then used throughout all the mock-ups.
- **EMERALD Landing Page:** We developed a first version of how the EMERALD Landing Page could look like, as depicted in Figure 107.
- **Set-up an audit scope**: We drew first mock-ups about how an EMERALD audit scope (previously called target of evidence) could be set up, as shown in Figure 108.
- **Overview of an audit scope**: After having created an audit scope, we prepared some mock-ups of what the audit scope overview page might look like as, presented in Figure 109.
- **Managing individual controls**: We developed mock-ups showing the respective information per control, including an overview of the control, evidence, non-compliance, metric, assignment, and history, as presented in Figure 110.

Be aware, that in this first set of mock-ups only the needs of the pilot partners were considered. Up to this point, we had not talked in detail with the component owners, consequently these mock-ups did not yet represent the needs of each component, nor their functionalities and features. This means that the mock-ups presented below were not completed and needed further refinements and continuous design iterations.

Figure 106 presents the first idea of the EMERALD design, considering the overall EMERALD project design and the colour palette designed of the project.

Figure 106. Paper-based Mock-ups – EMERALD Design

Figure 107 presents the landing page which should provide direct access to the most relevant functionalities and features of EMERALD, including the respective EMERALD components. In the first draft, we added all EMERALD components explicitly here, however, as the EMERALD UI should be an integrated UI including all EMERALD components, this would be changed.

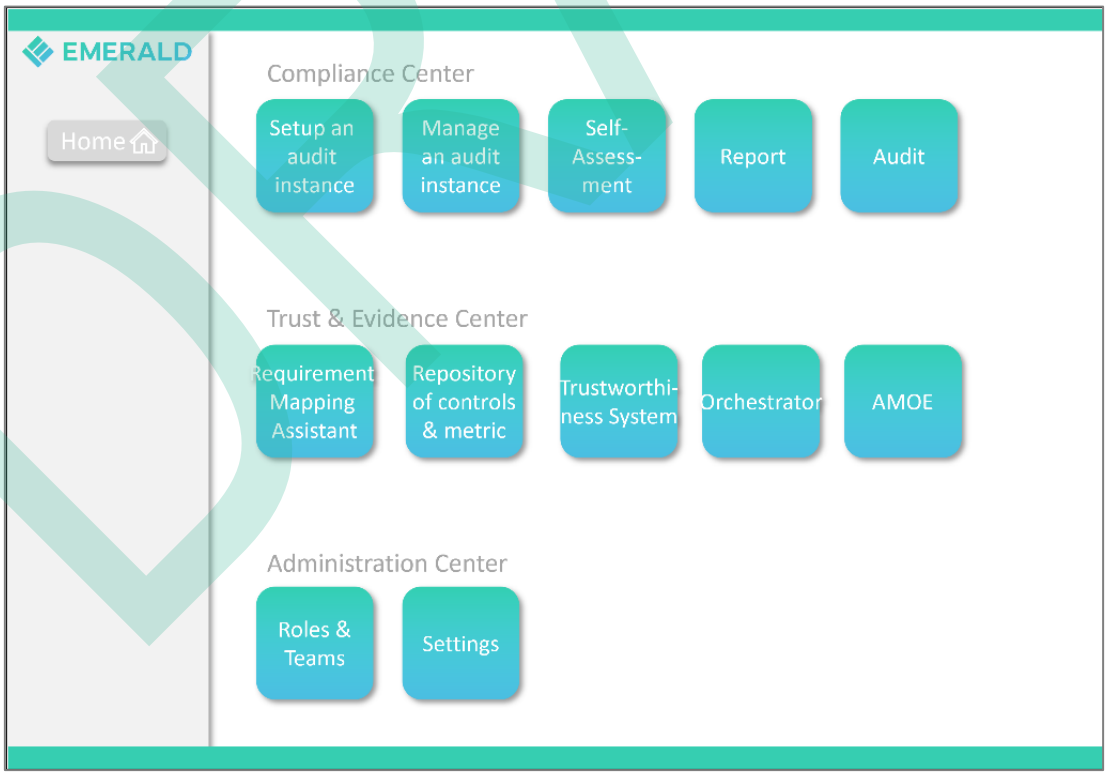

Figure 107. Paper-based Mock-ups – EMERALD Landing Page

Figure 108 shows the initial version of how-to setup an audit scope (still called “audit instance” in the mock-up). In addition to naming the audit scope, it allows the user to select a predefined cloud service and the respective certification scheme (still called “standard” in the mock-up). Furthermore, it is possible to upload policy documents. What is missing is the relation to the technical evidence, which would be addressed at a later stage.

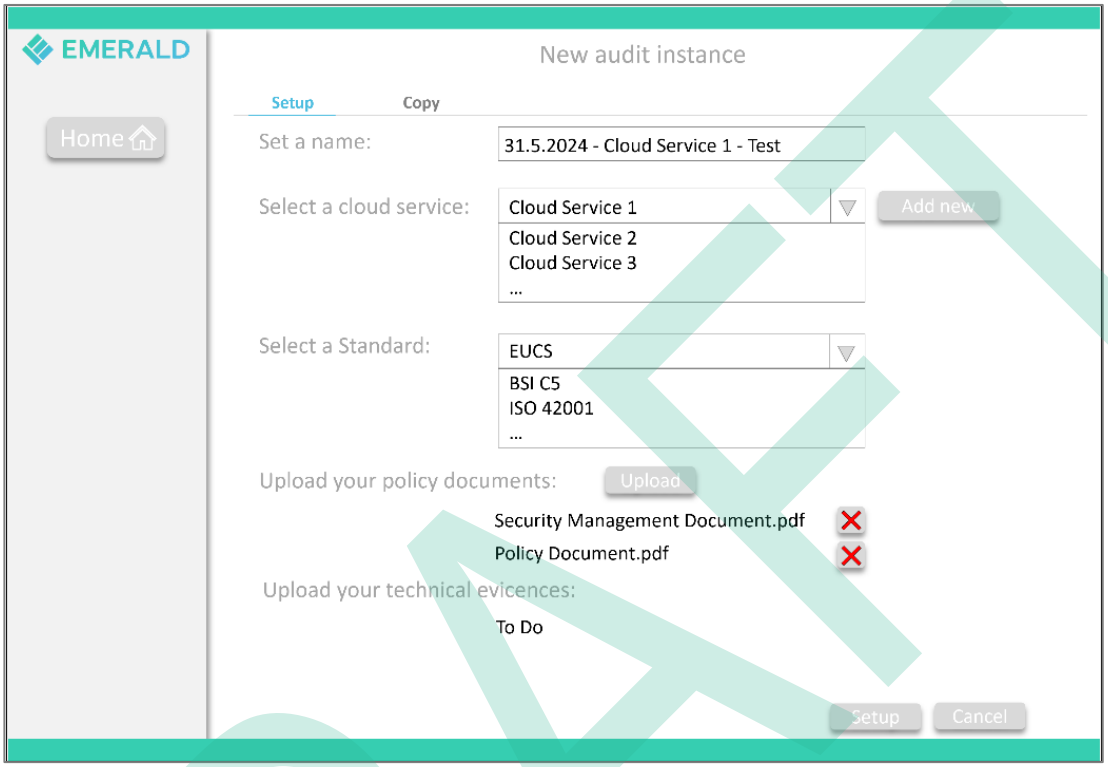

Figure 108. Paper-based Mock-ups – Setup of a new audit scope

Figure 109 shows what the overview page for an audit scope might look like. On top it presents information regarding the audit scope, the selected certification target (still called “cloud service” in the mock-up), the certification scheme (called “standard” in the mock-up) and the assurance level. Below it provides some boxes with overview information about the compliance and non-compliance states across all controls, general status information about the individual controls as well as a box regarding the upload of the policy documents. Below it presents a search bar allowing to search for specific controls and then presents a list of the categories and controls of the respective certification schemes, functionalities for filtering the list and accessing the individual controls.

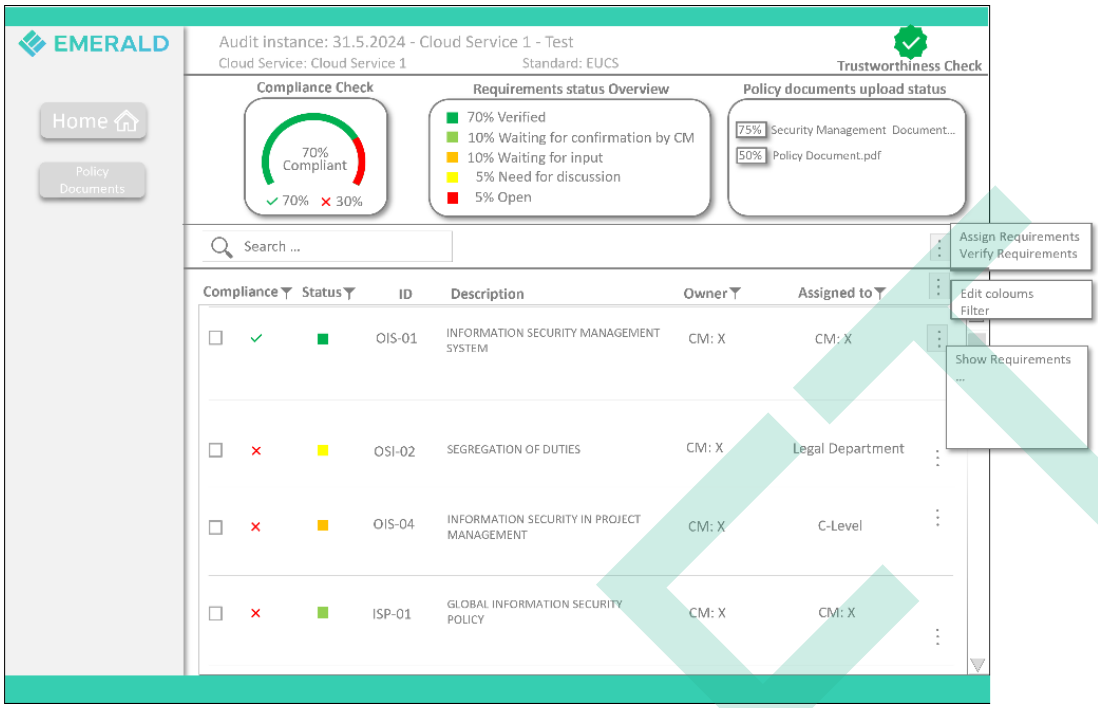

Figure 109. Paper-based Mock-ups – Audit scope overview

Figure 110 presents a detailed view of a control. Information about the audit scope and the control are on top of the mock-up. Below a user can switch via several “tabs” to the different information including: i) overview of the control - presenting some general information, ii) evidence – showing the pieces of evidences extracted for the control, iii) non-compliance – if this control would be non-compliant, the reasons would be presented here, iv) metric information – presents which metrics were assigned to the control, v) assignment information – showing information on who is responsible for the control, vi) and a history – showing how the implementation of the control has evolved over time.

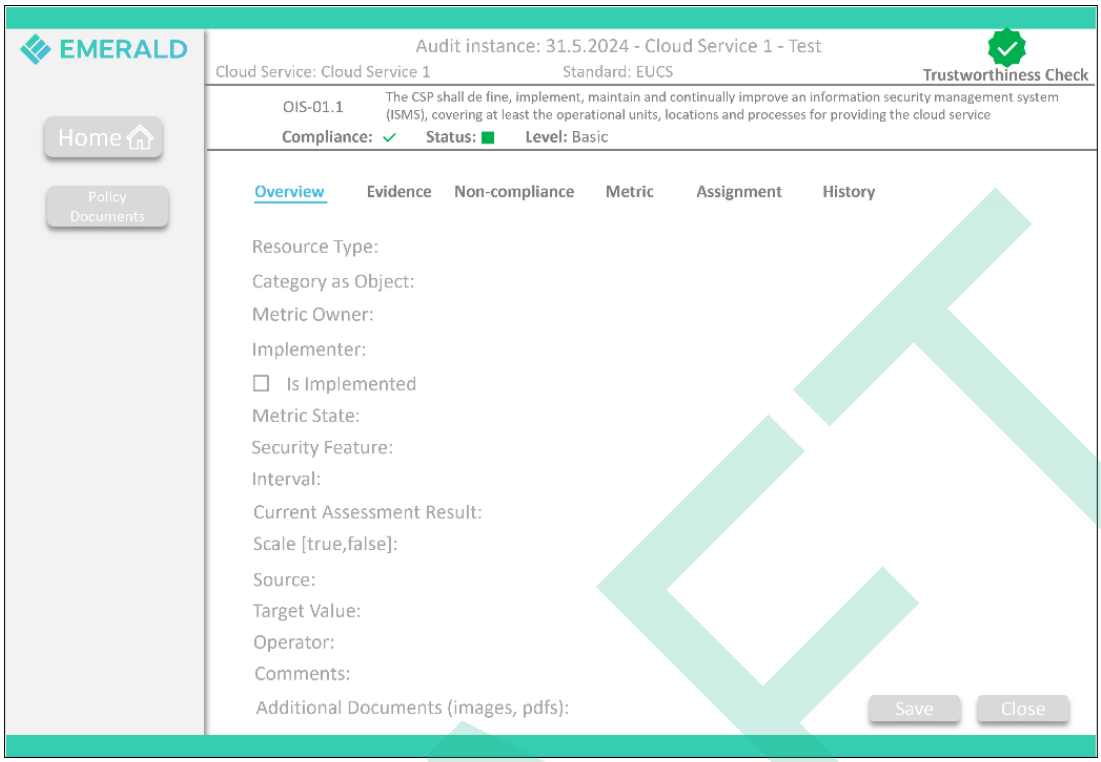

Figure 110. Paper-based Mock-ups – Show information about a control

Further mock-ups can be found in the APPENDIX B: Mock-ups derived from the interviews and APPENDIX C: User Journeys and paper-based Mock-ups.

9 APPENDIX B: Mock-ups derived from the interviews

In this appendix, we present all other mock-ups that we have derived from the interviews with pilot partners, including a short description for each of them.

9.1 Mock-ups for managing an audit scope

In the following we present several mock-ups for managing audit scopes. Figure 111 presents the possibility to select an existing audit scope.

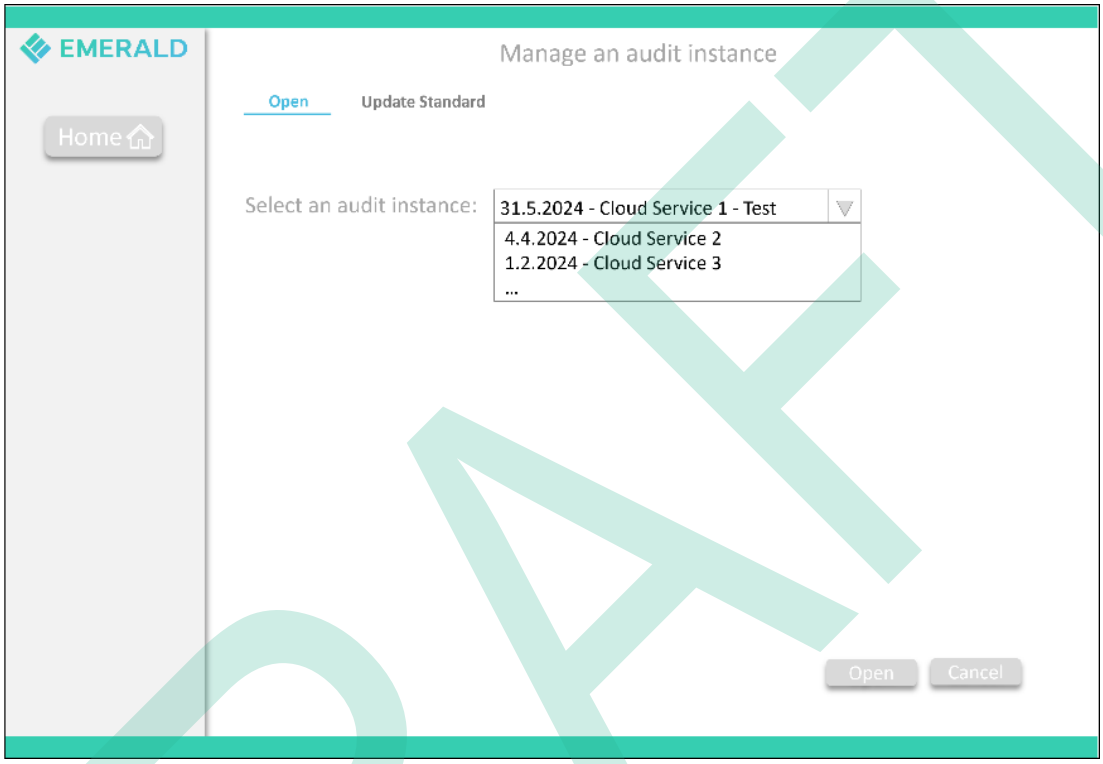

Figure 111. Paper-based Mock-ups – Open an existing audit scope

Figure 112 presents a mock-up on how to update an existing audit scope when a new certification scheme is available.

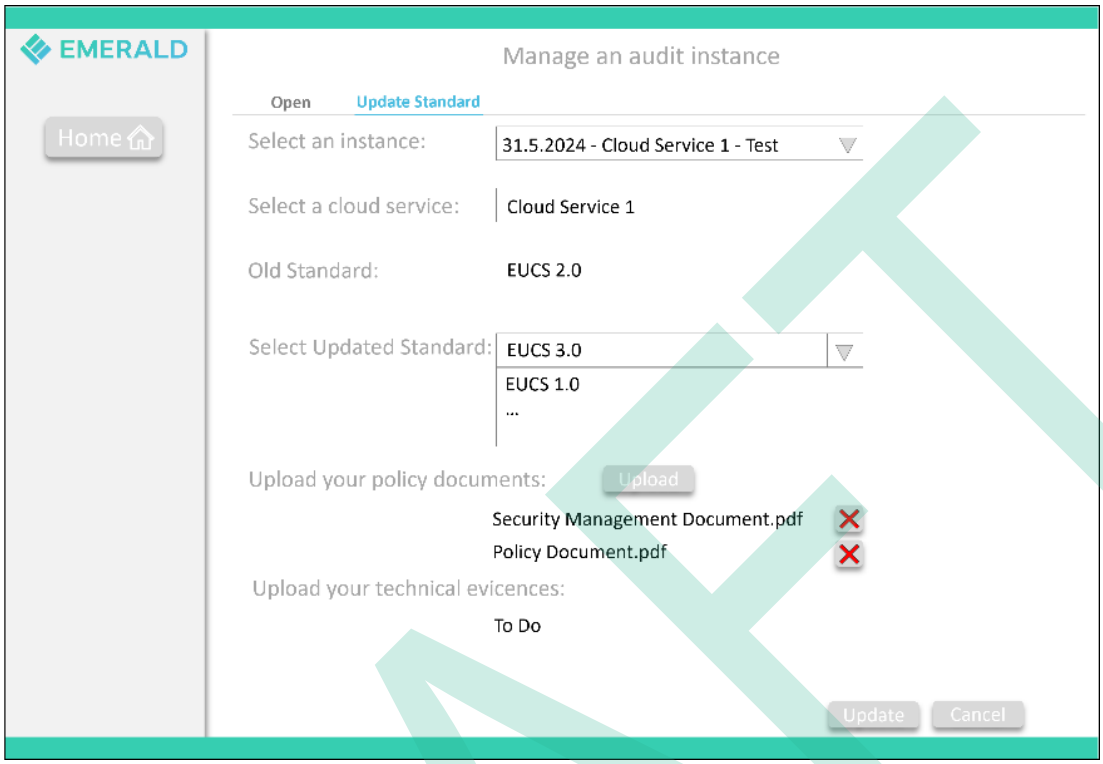

Figure 112. Paper-based Mock-ups – Update the certification scheme of an existing audit scope

Figure 113 presents a mock-up that allows to copy an existing audit scope to create a new one.

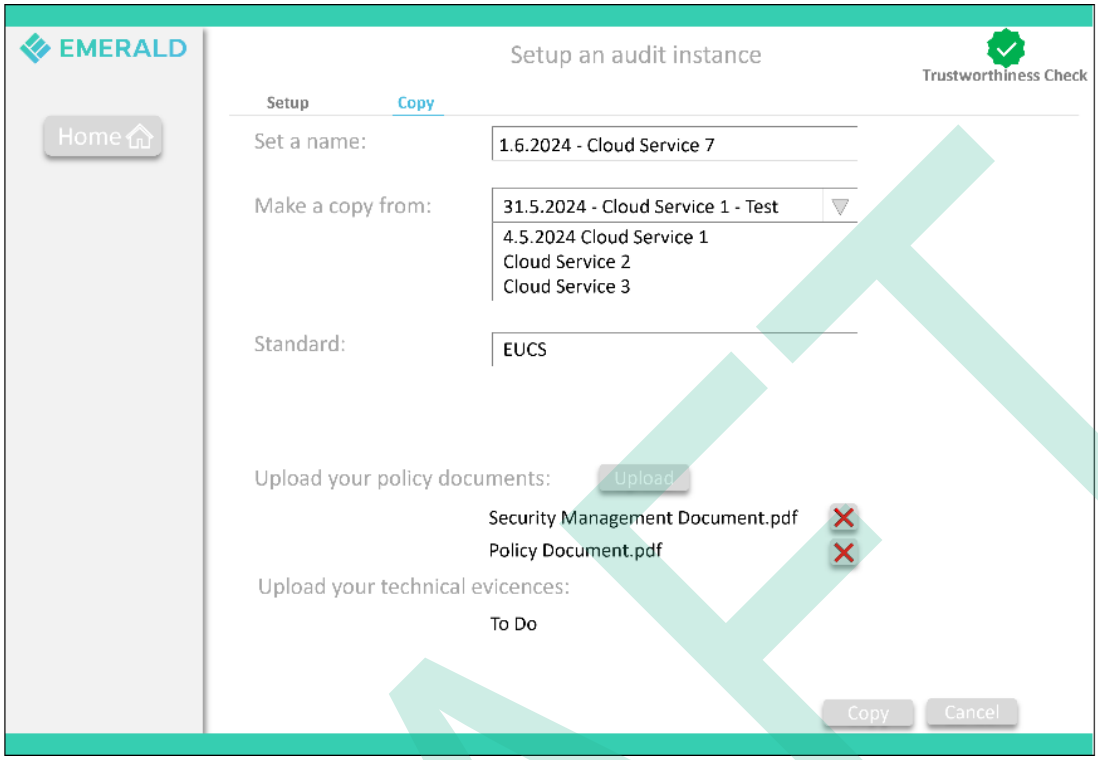

Figure 113. Paper-based Mock-ups – Make a copy of an existing audit scope

9.2 Mock-ups presenting the overview of an audit scope

In the following, several mock-ups are presented on what an overview page of a selected audit scope might look like.

Figure 114 presents an overview of an audit scope showing the categories of EUCS as an example. Clicking on a category would show the corresponding controls of the category.

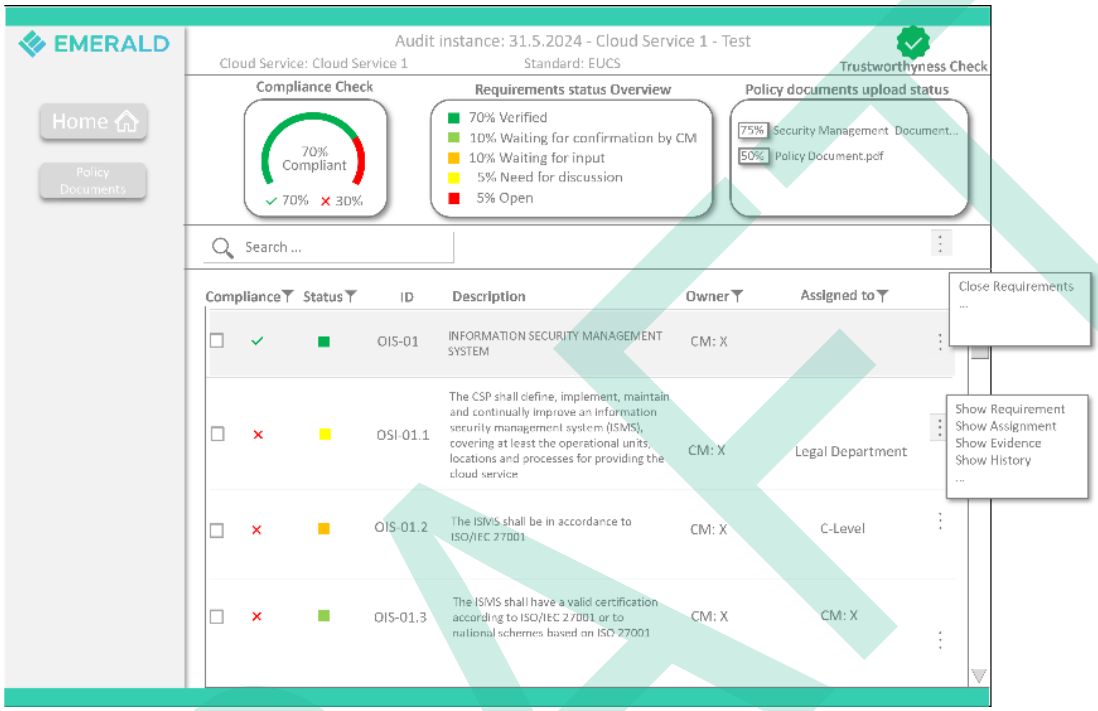

Figure 114. Paper-based Mock-ups – Show overview of a category and the respective controls

Figure 115 presents the overview of an audit scope showing only controls (without any categories).

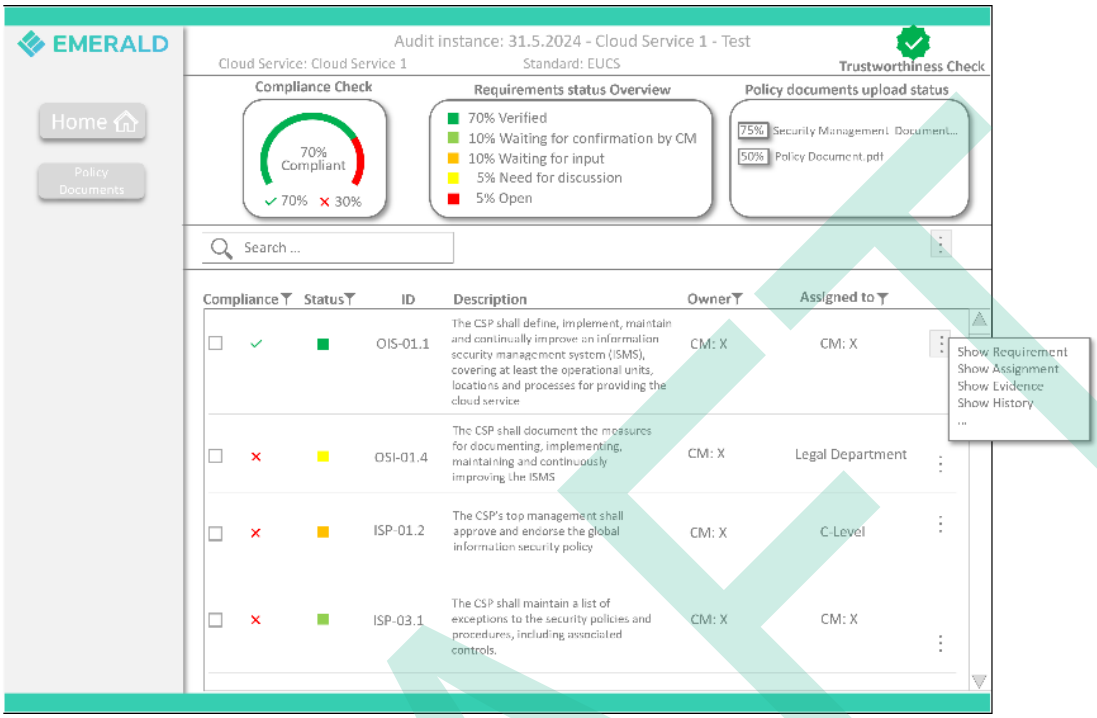

Figure 115. Paper-based Mock-ups – Show an overview of the controls only (no categories)

9.3 Mock-ups presenting the controls

In the following, several mock-ups are presented showing which information could be presented regarding individual controls of a certification scheme.

For each control a lot of information needs to be shown. Figure 110 in APPENDIX A: Mock-ups derived from Interviews with Pilot Partners presents an example of showing some general information about a control. Figure 116 shows how possible evidence extracted for the current control could be presented where organisational and technical evidence is divided into two

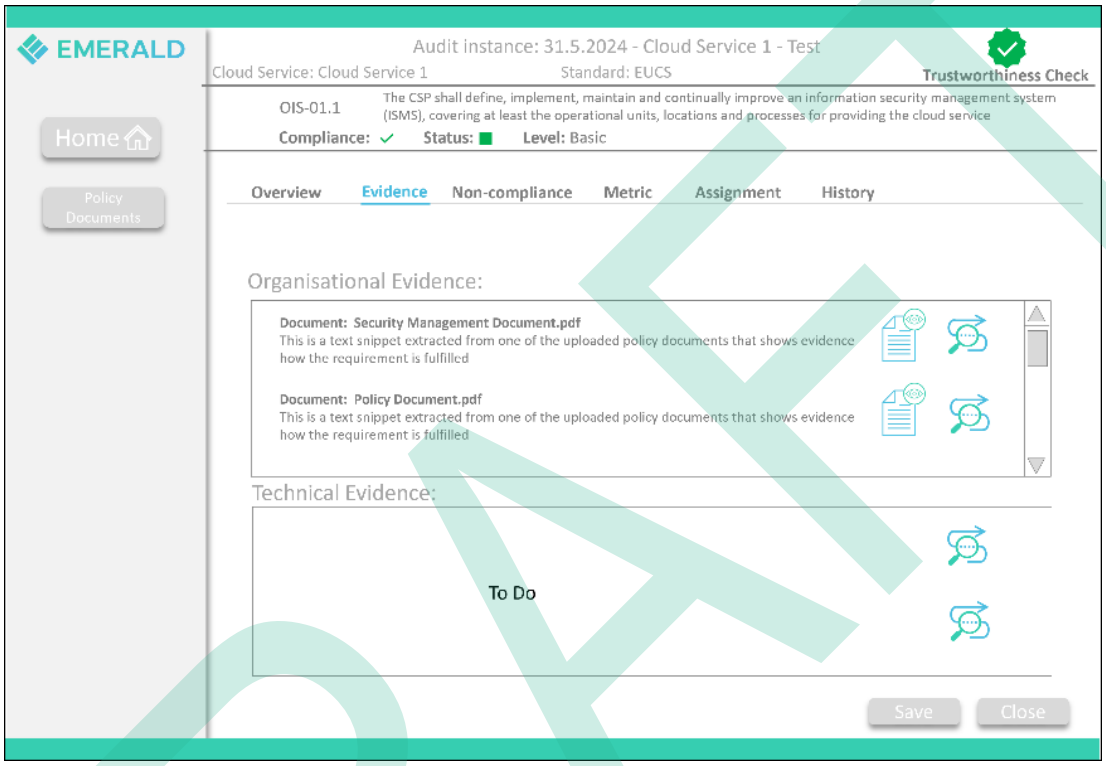

Figure 116. Paper-based Mock-ups – Suggestion – Different types of evidence for control (v1)

parts.

Figure 117 shows how possible evidence extracted for the current control could be presented, where organisational and technical evidence are shown in a combined view.

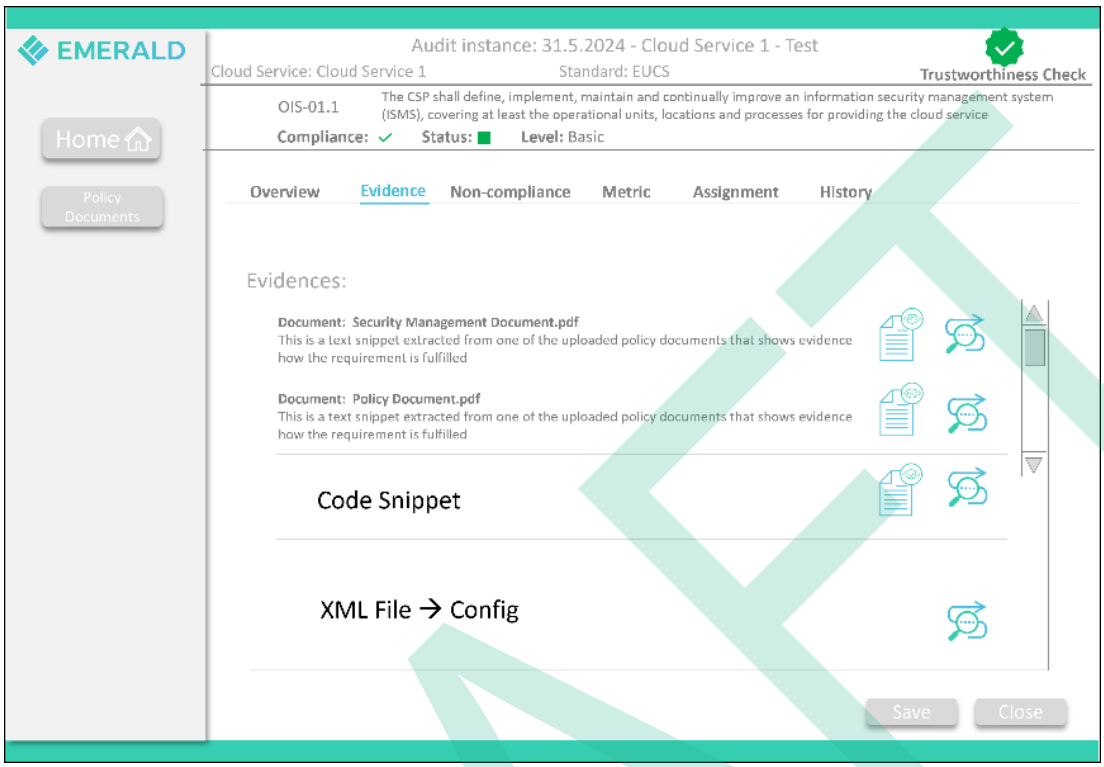

Figure 117. Paper-based Mock-ups – Suggestion: Different type of evidence for control (v2)

Figure 118 presents a suggestion of how information on possible non-compliances detected can be presented for the respective control.

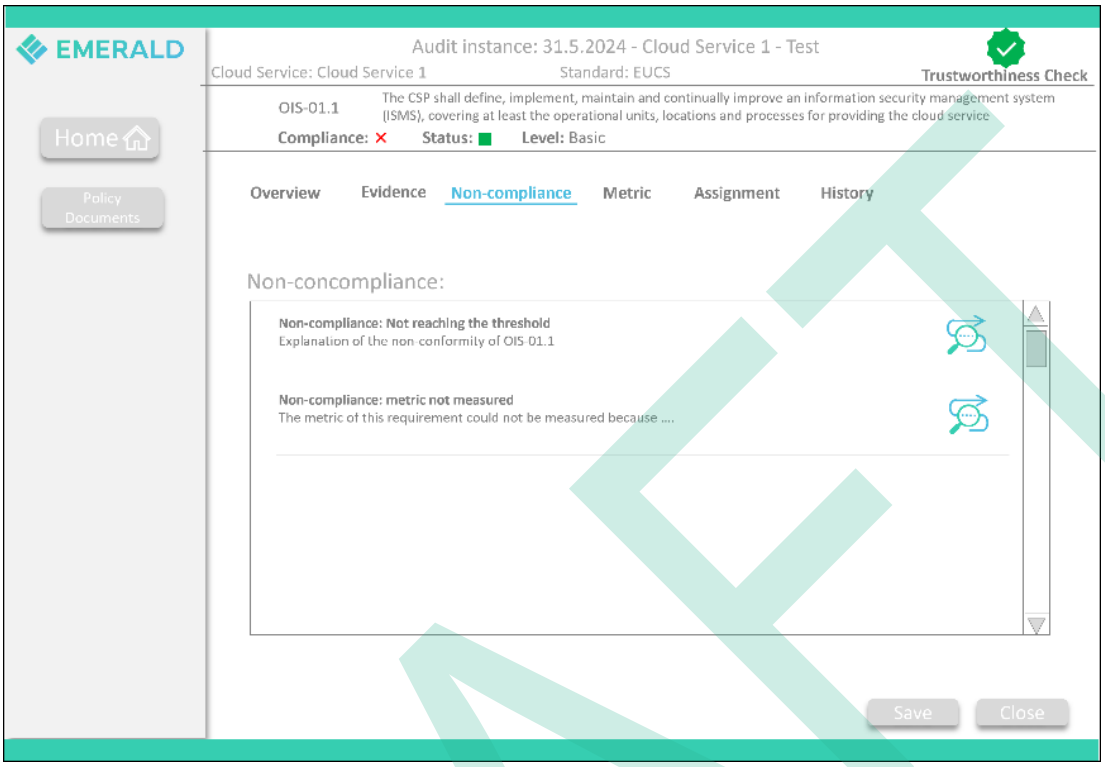

Figure 118. Paper-based Mock-ups – Suggestion: Information about non-compliances

Figure 119 presents a mock-up of what an assignment of a control to either an individual person or to a whole department might look like.

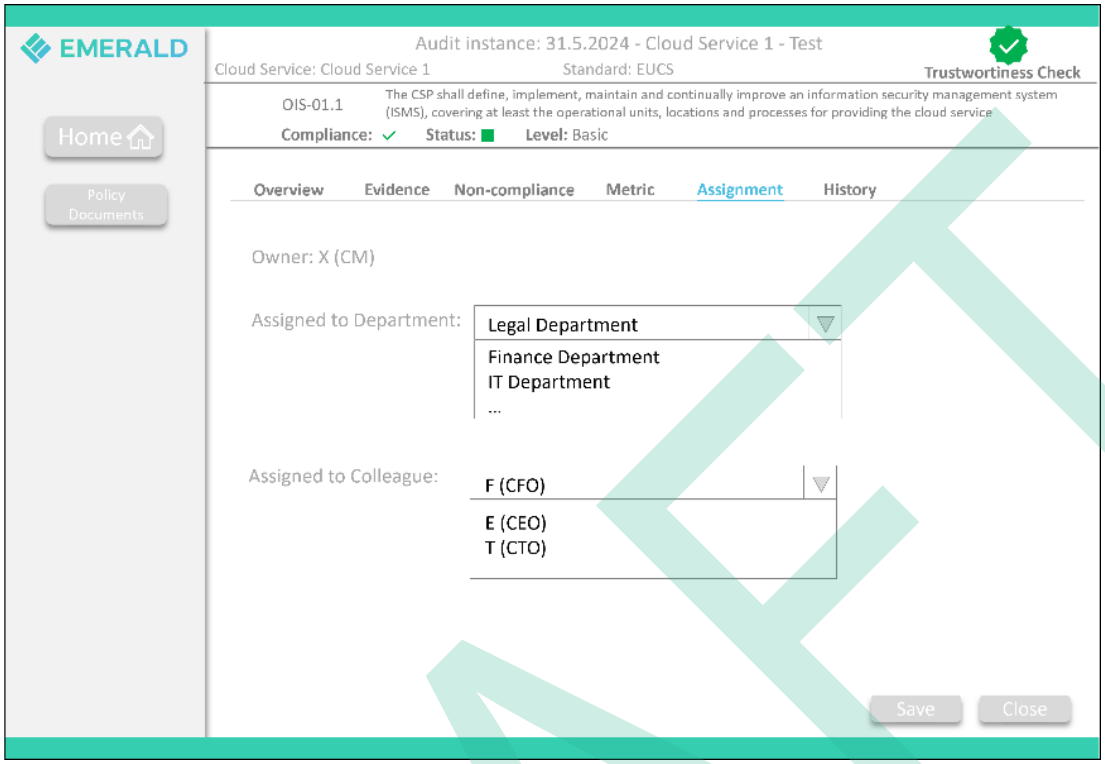

Figure 119. Paper-based Mock-ups – Suggestion: Assign a control to a colleague/department

Figure 120 shows what a control history, showing all changes of the control, might look like in the EMERALD UI.

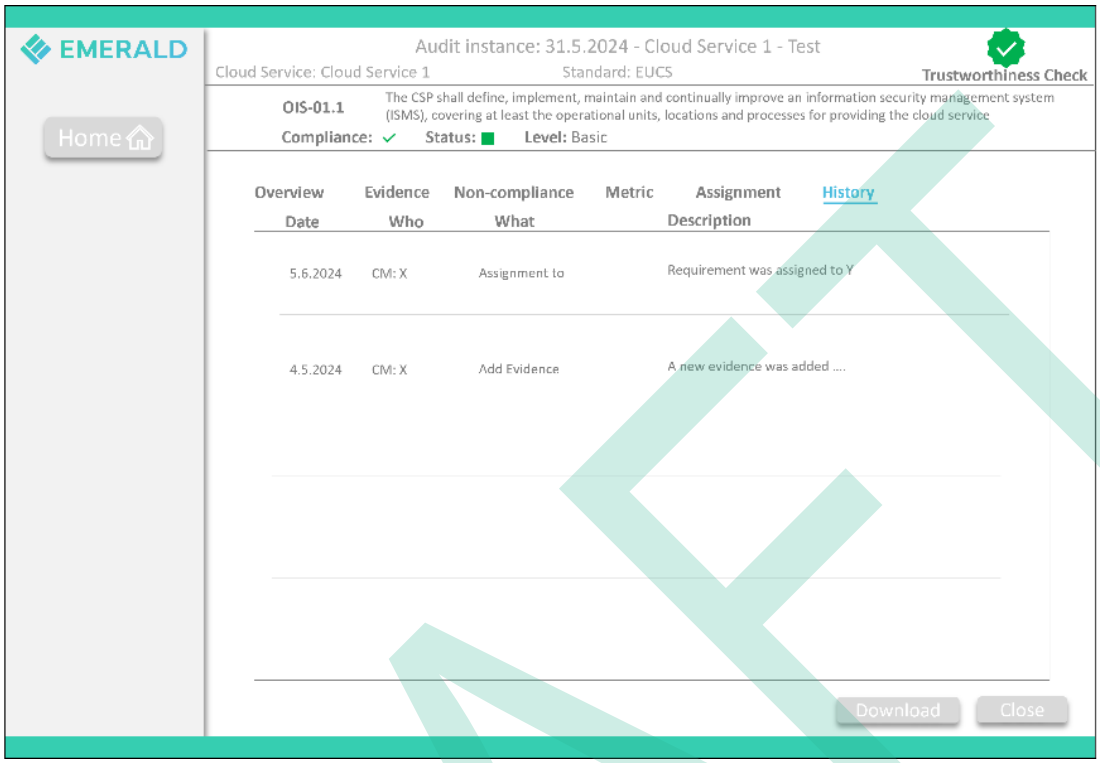

Figure 120. Paper-based Mock-ups – Suggestion: History information of a control

10 APPENDIX C: User Journeys and paper-based Mock-ups

Based on the personas and scenarios, user journeys were developed. To do so, each scenario was divided into different steps. Thereby, each step was divided into two sections. The first section consists of the description of the task the persona would like to do according to the scenario. And the second section describes the desired interaction with the EMERALD UI, including the relevant functionalities that the EMERALD UI should offer to be able to conduct the task.

In the following sections, we first describe in detail the user journey, and then the resulting paper-based mock-ups.

10.1 User Journey 1: Emerson – Bring your own certification scheme.

The scenario for Emerson was divided into the following six step, as depicted in Figure 121. For each step, first Emerson's task is described and then the interaction with the EMERALD UI.

Step 1:

- **Emerson's Task**: 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.
- **Interaction with the EMERALD UI**: no interaction required.

Step 2:

- **Emerson's Task**: 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). Emerson selects the set of controls from the available certification schemes. Emerson would also like to define their own controls.
- **Interaction with the EMERALD UI**: Emerson enters the EMERALD tool, selects the certification schemes tab, chooses the "new certification scheme" option, and enters a name for it. Emerson then selects a list of controls from different certification schemes. Additionally, Emerson also wants to define their own controls. Then they save the scheme.

Step 3:

- **Emerson's Task**: Emerson creates an audit scope that will be used for managing cloud solutions and the respective BYOCS standard.
- **Interaction with the EMERALD UI**: Emerson goes to EMERALD tab for creating a new audit scope (target of evaluation) and selects the previous tailored certification scheme of Step 1.

Step 4:

Emerson's Task: Emerson opens the EMERALD solution, selects the audit scope and the XYZ cloud solution to be audited, and uploads all relevant documents (and links, ...) to be able to get the respective evidence for some of the controls.

- **Interaction with the EMERALD UI**: Emerson selects the audit scope and the provider XYZ and starts uploading evidence.

Step 5:

- **Emerson's Task**: Emerson's task is now to go through all controls to check if all of them can be met with some evidence (technical or organisational).
- **Interaction with the EMERALD UI**: Emerson goes to EMERALD UI and visualizes the evidence linked with the control and the overall compliance in a first automatic iteration.

Step 6:

- **Emerson's Task**: Emerson goes to the EMERALD UI to check the status of the controls regarding evidence and status. Emerson uses different functionalities available in the EMERALD UI like to filter controls and uses different visualisations of the overall status of all controls, etc., to find out which controls need some treatment, and which are already ok.
- **Interaction with the EMERALD UI**: Emerson goes to EMERALD UI and visualizes, filters, and manages the controls. Emerson can also extract metrics. Furthermore, from this view, Emerson must be able to follow the whole process to understand the decisions made.

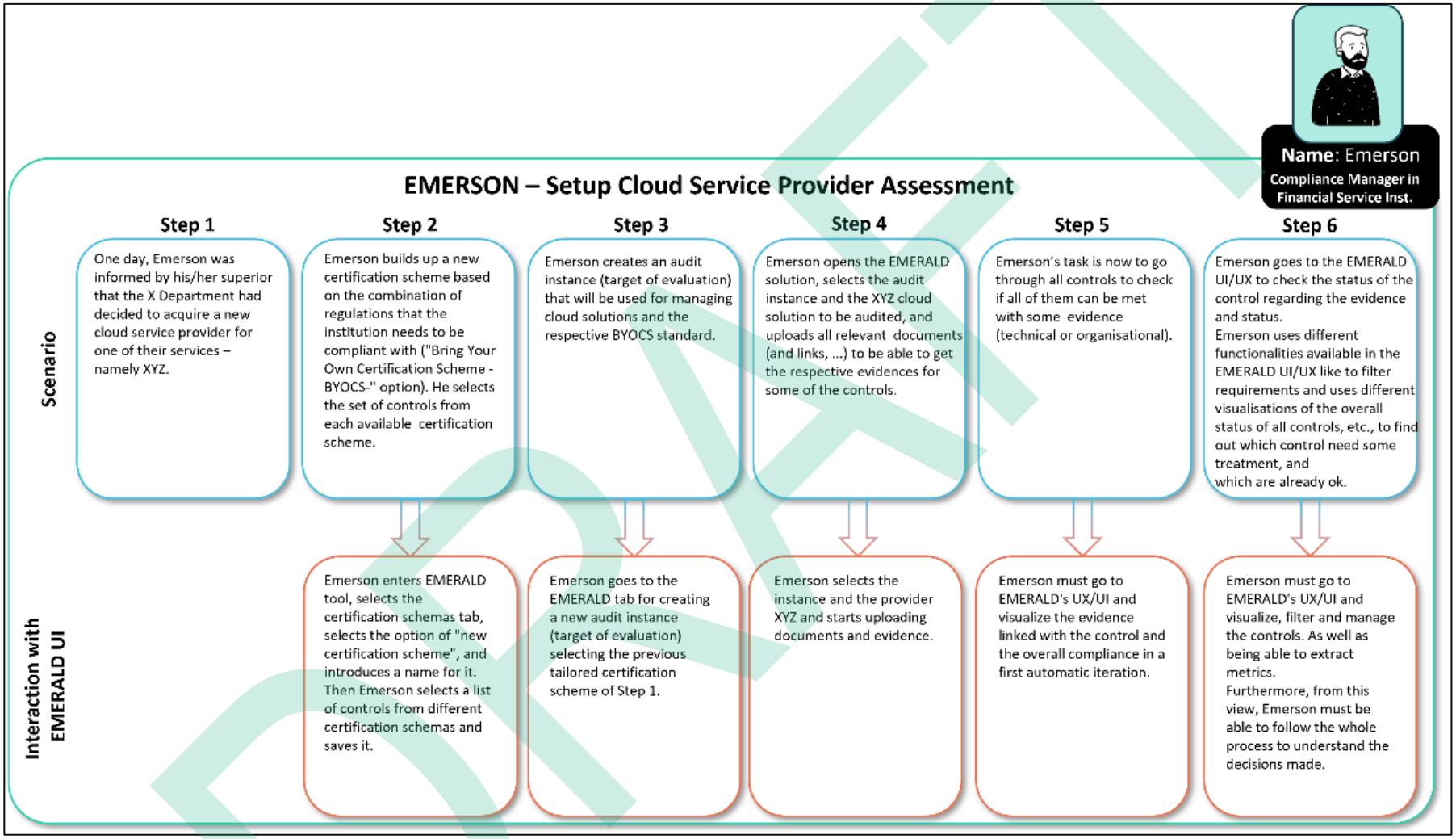

Figure 121. User Journey 1: Emerson – Bring your own certification scheme

10.1.1 Mock-ups: Emerson – Bring your own certification scheme

Based on the user journey, we have created a set of mock-ups that maps parts of the user journey to the mock-ups. In the case of user journey 1, we present the mock-ups for creating a new certification scheme (Step 2), where Emerson can select different controls from different schemes. Additionally, the mock-ups present how to select for a new audit scope the newly developed scheme (Step 3).

Figure 122 shows that an BYOCS ("Bring your own certification scheme") was added to the landing page of the EMERALD UI.

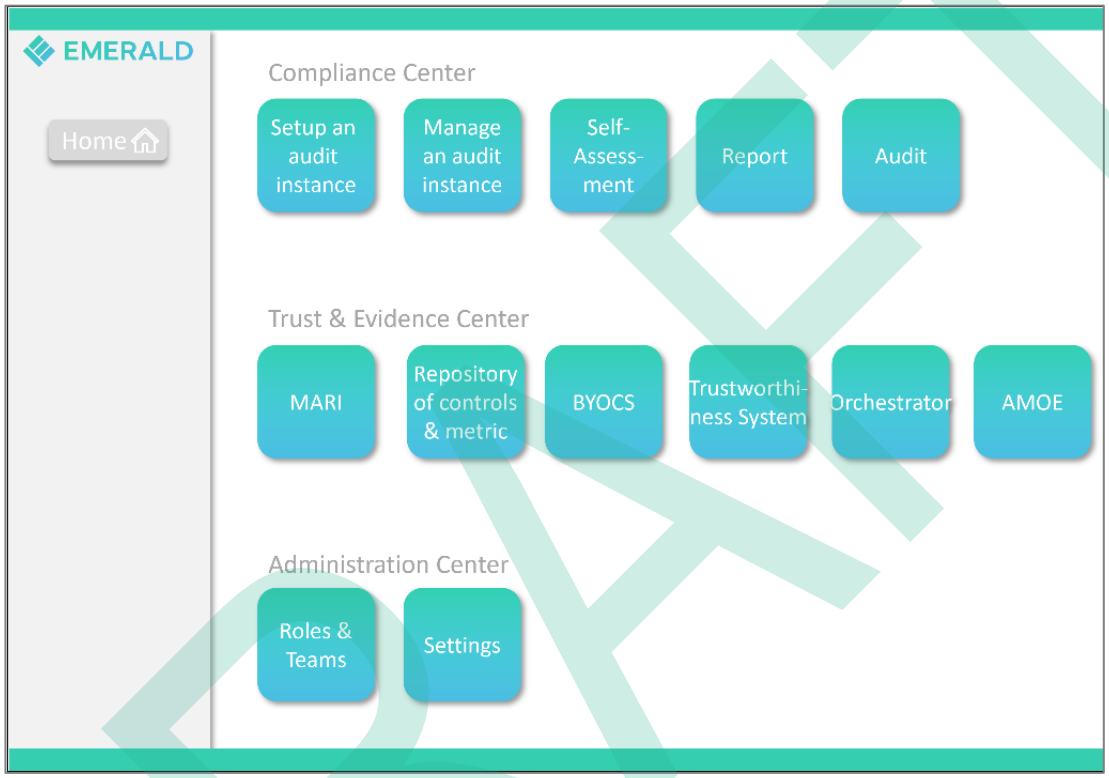

Figure 122. Paper-based Mock-ups – User Journey 1 – Step 2: Add BYOCS to Landing Page

Figure 123 asks Emerson to add a name for the new scheme and to choose those certifications schemes from which they would like to use the controls from to create a new scheme.

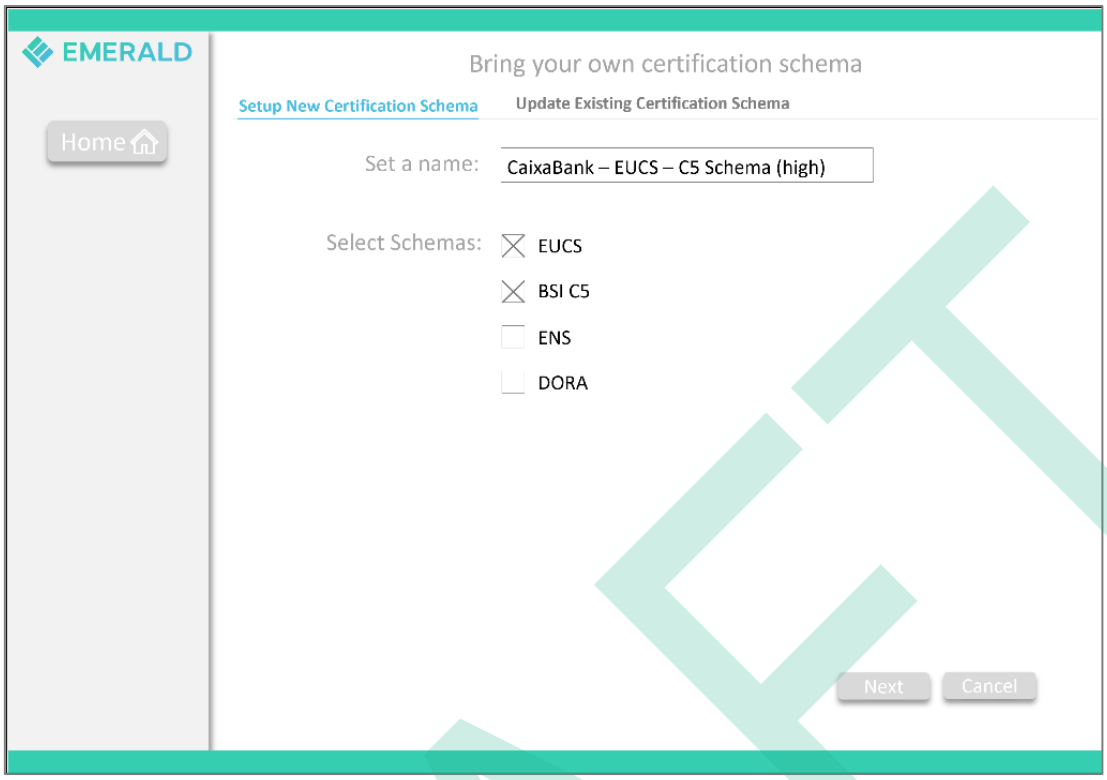

Figure 123. Paper-based Mock-ups – User Journey 1 – Step 2: Scheme name and schemes

Figure 124 shows the user interface that allows to select different controls including their respective metrics assigned from existing certification schemes like EUCS or BSI C5 to the new certification scheme.

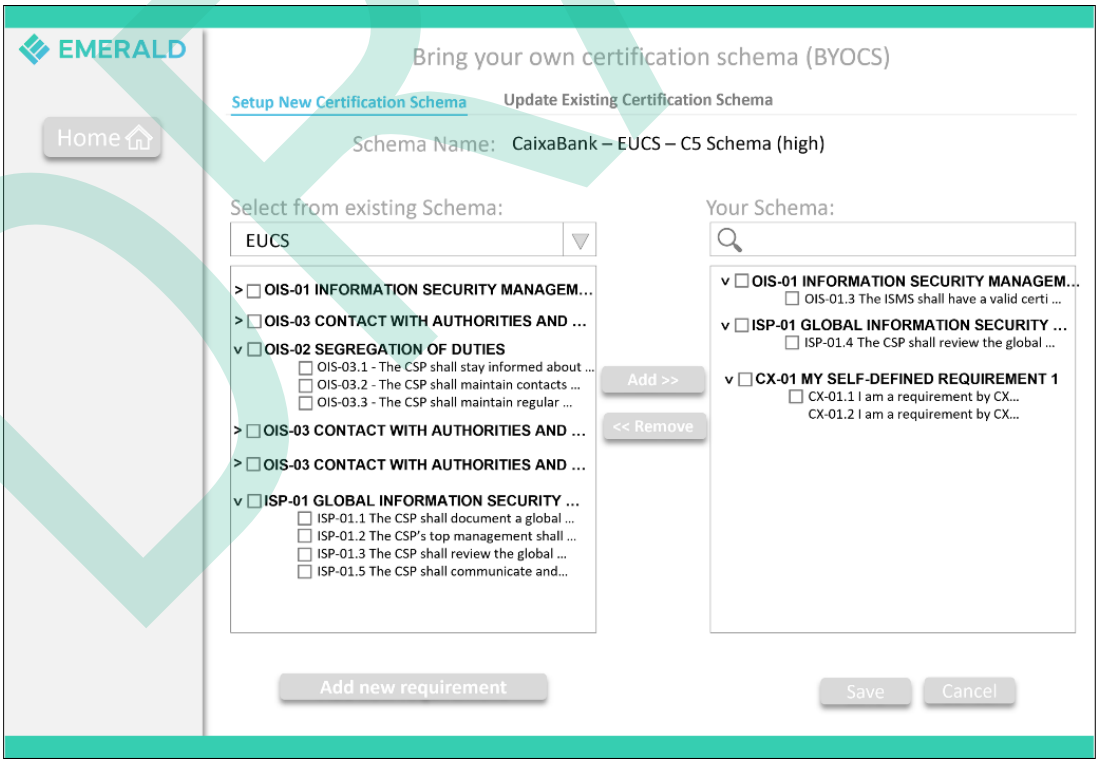

Figure 124. Paper-based Mock-ups – User Journey 1 – Step 2: Add controls to new scheme

Figure 125 presents the possibility to add a new self-defined control.

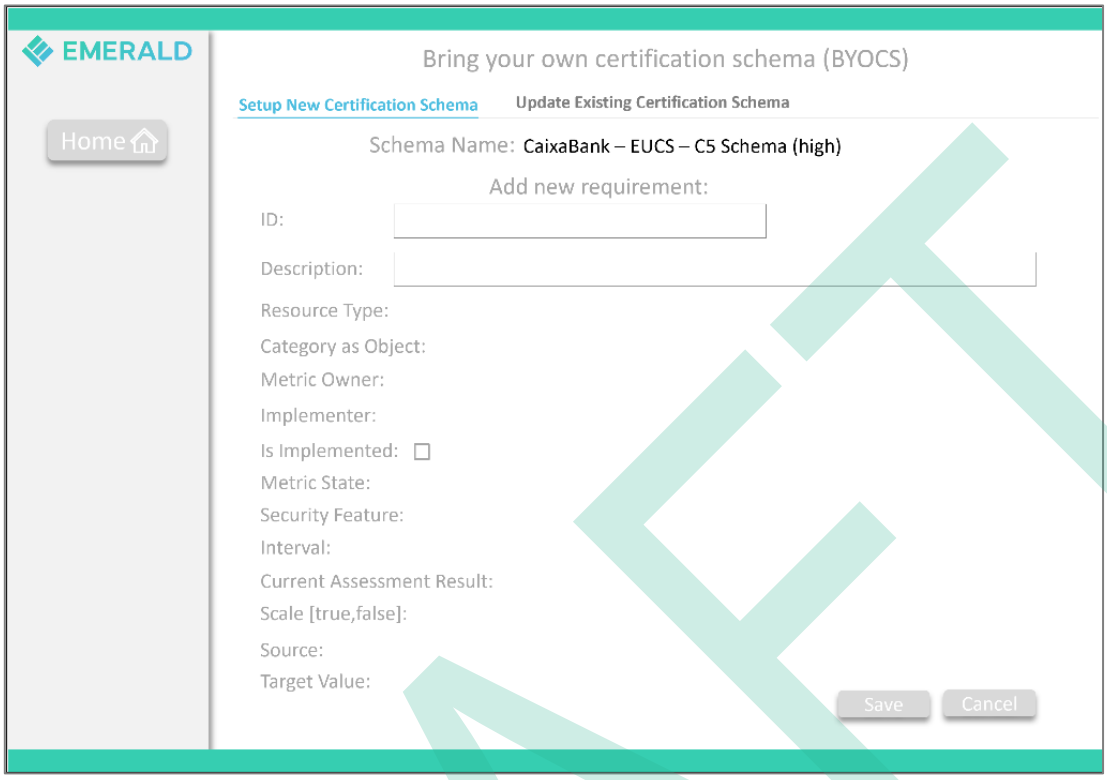

Figure 125. Paper-based Mock-ups – User Journey 1 – Step 2: Define own control

Figure 126 presents how to select the newly created scheme for setting up a new audit scope.

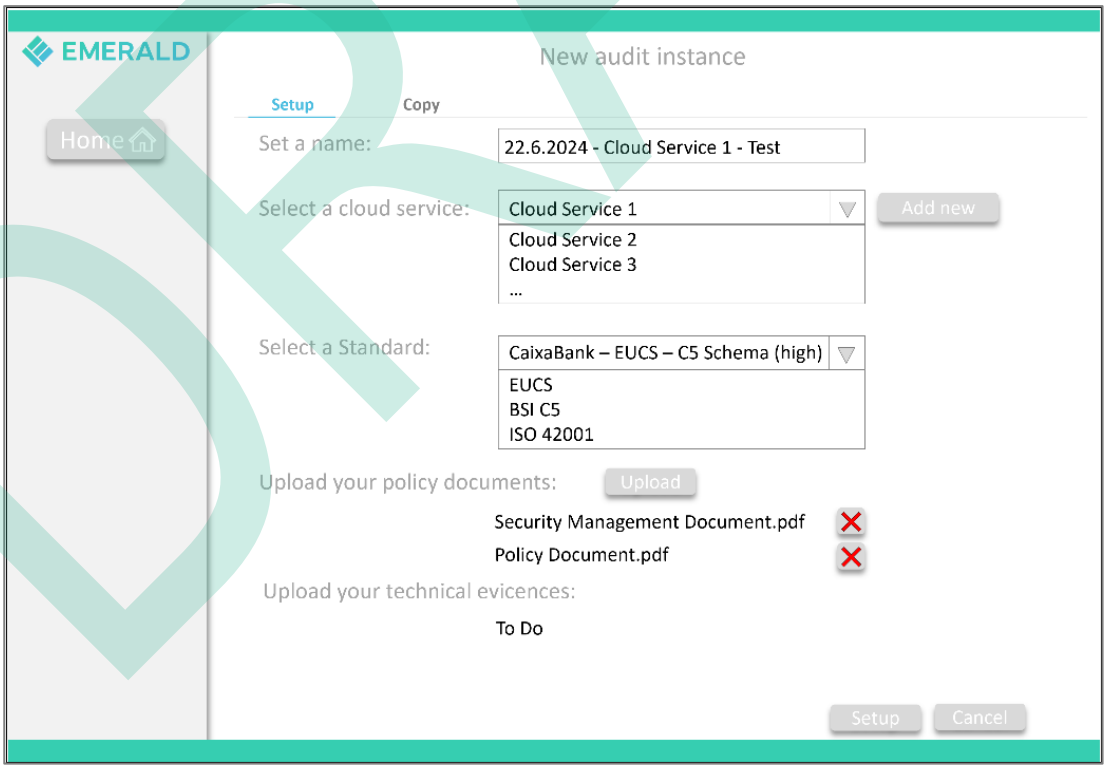

Figure 126. Paper-based Mock-ups – User Journey 1 – Step 3: Select new scheme for audit scope

10.2 User Journey 2: Dylan – Internal Control Owner Control Implementation

The scenario for Dylan was also divided into six steps, as depicted in Figure 127. For each step, first Dylan's task is described and then the interaction with the EMERALD UI.

Step 1:

- **Dylan's Task**: Dylan opens the EMERALD UI to check if there are any new controls that need to be worked on.
- **Dylan's Interaction with the EMERALD UI**: Dylan opens the EMERALD UI in their web-browser and signs in with their credentials. They are then redirected to the EMERALD Dashboard where all assigned controls can be easily seen.

Step 2:

- **Dylan's Task**: If Dylan finds a new control, but they cannot provide the evidence by themselves, they assign it to colleague Y.
- **Dylan's Interaction with the EMERALD UI**: In the detail view of a control, Dylan assigns a colleague of theirs as its implementer. EMERALD notifies their colleague about a new control.

Step 3:

- **Y's Task:** Y views the personal control Todo list.
- **Y's Interaction with the EMERALD UI:** Y navigates to their personal control overview and opens the detailed view of a control.

Step 4:

- **Y's Task**: Y checks if there are already recommended metrics that can be used. Y assigns the metrics to the control.
- **Y's Interaction with the EMERALD UI:** Y opens the MARI tool and selects a set of metrics for the control.

Step 5:

- **Y's Task**: Y checks all metrics for their implementation status. If they are not yet implemented, they are assigned.
- **Y's Interaction with the EMERALD UI**: Y can see the implementation status of the necessary metrics in the overview of the control. If they are not yet implemented, they can also be assigned to another colleagues – colleague Z - in the view.

Step 6:

- **Z's Task**: Z implements the metric and makes sure the evidence is included in the EMERALD solution.
- **Z's and Dylan's Interaction with the EMERALD UI**: Z sees the list of metrics to be implemented. Z implements the metric and confirms the implementation once it is done. Dylan gets notified about the new status of the control. The dashboard is updated. Dylan sees the new status of their controls.

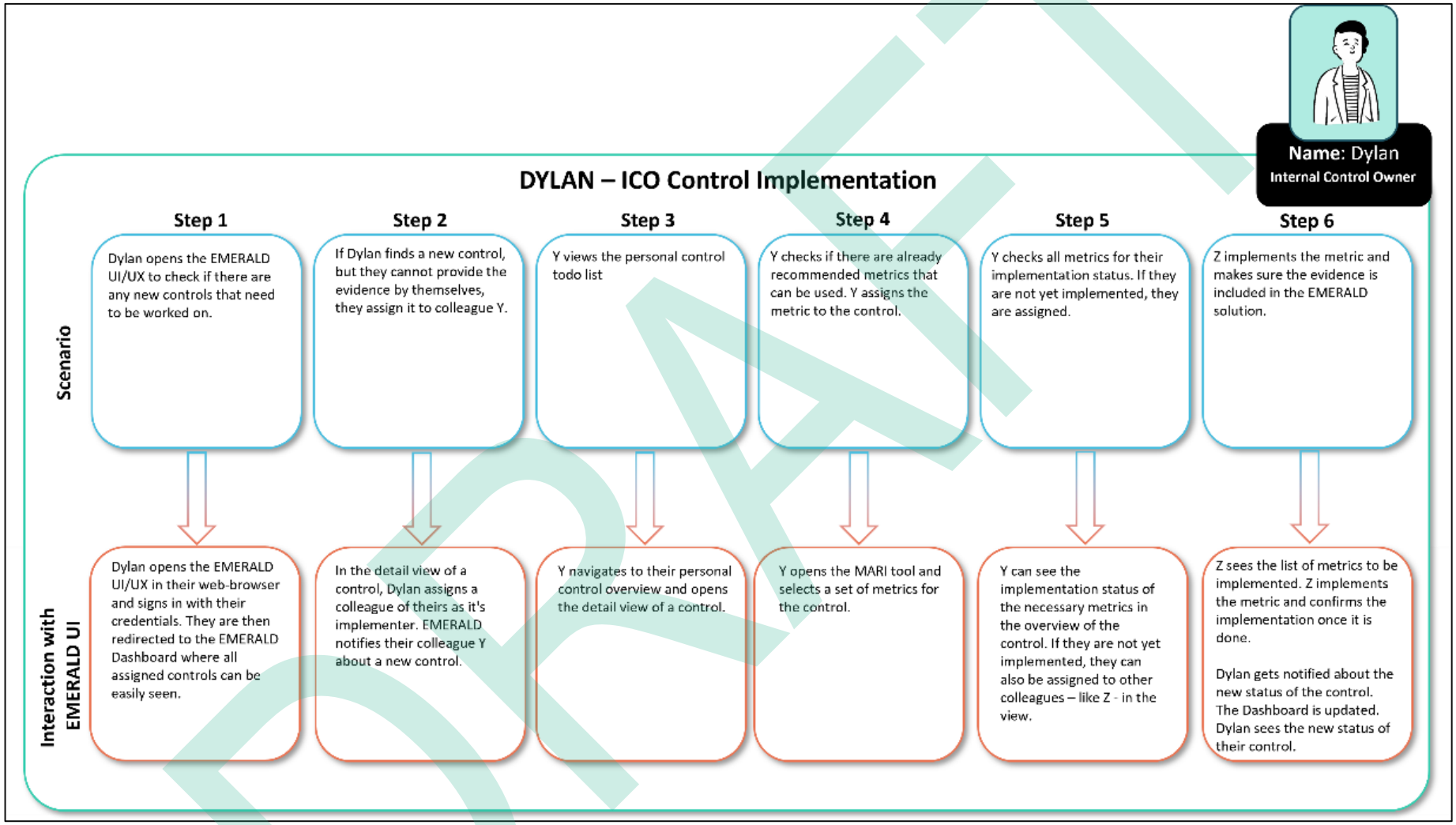

Figure 127. User Journey 2: Dylan – ICO Control Implementation

10.2.1 Mock-ups: Dylan – Internal Control Owner Control Implementation

Based on the user journey from Dylan, we have created a set of mock-ups that maps parts of the user journey to the mock-ups. In the case of user journey 2, we focus on the mock-ups for filtering for non-compliant controls (Step 1) and for assigning an open control to a colleague (Step 2).

Figure 128 shows how to select an existing audit scope.

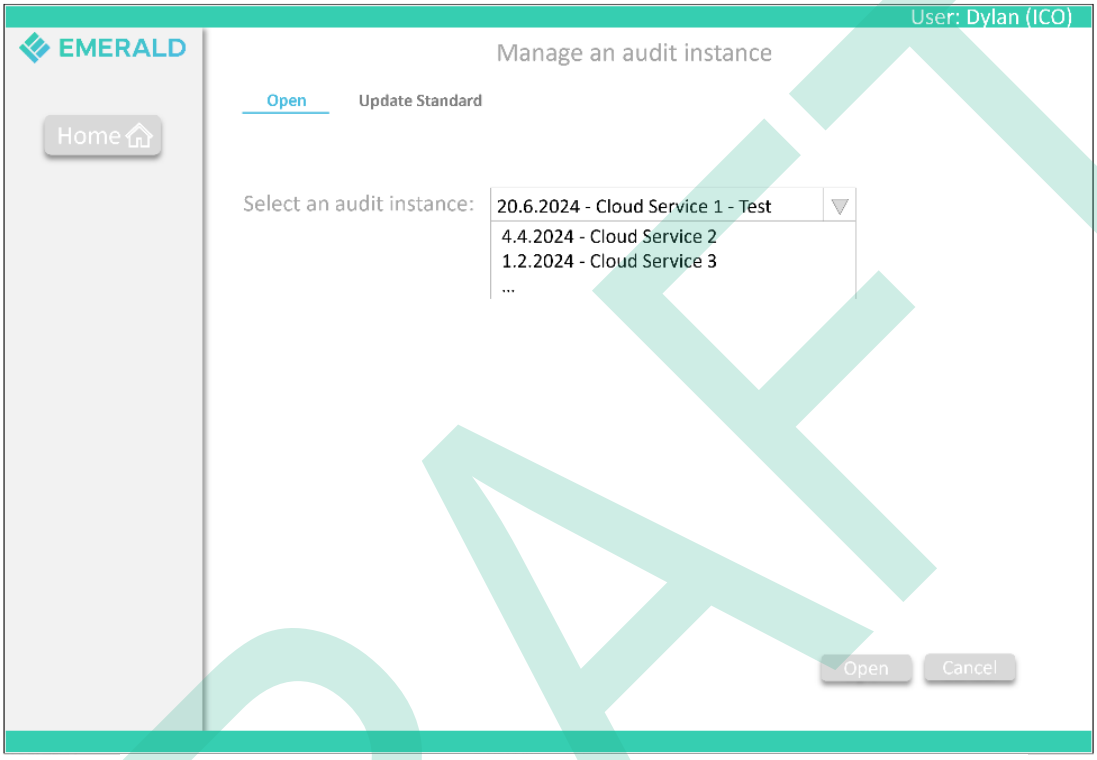

Figure 128. Paper-based Mock-ups – User Journey 2 – Step 1: Open an existing audit scope

Figure 129 presents the overview page of an existing audit scope and the list of the respective controls.

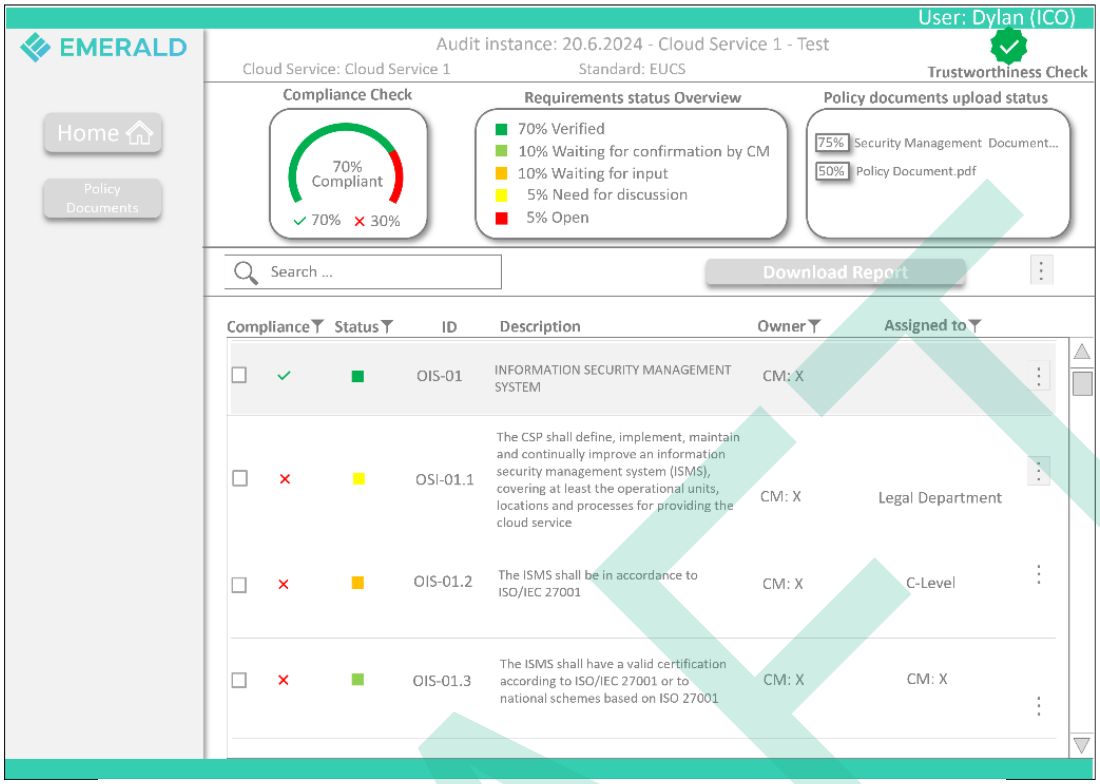

Figure 129. Paper-based Mock-ups – User Journey 2 – Step 1: Audit scope with list of controls

Figure 130 presents the overview of an audit scope and the possibility to filter for open controls – these are controls that have not been dealt with so far.

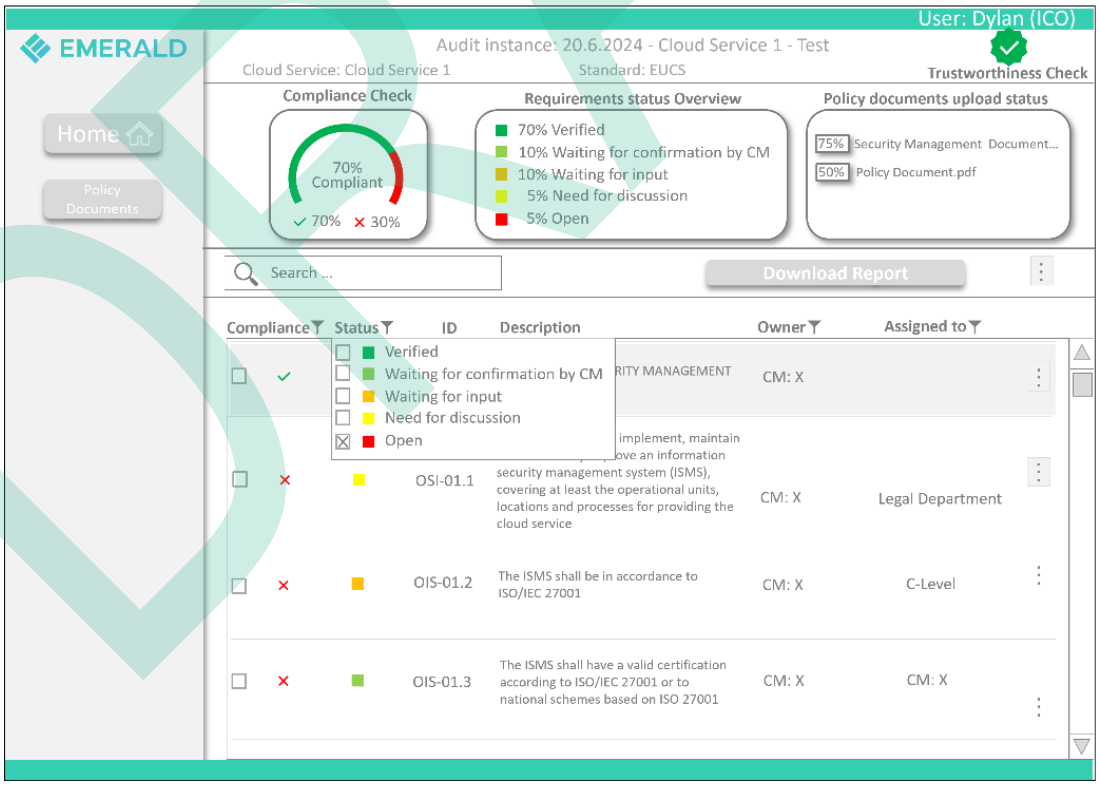

Figure 130. Paper-based Mock-ups – User Journey 2 – Step1: Filtering of controls

Figure 131 presents the list of open controls.

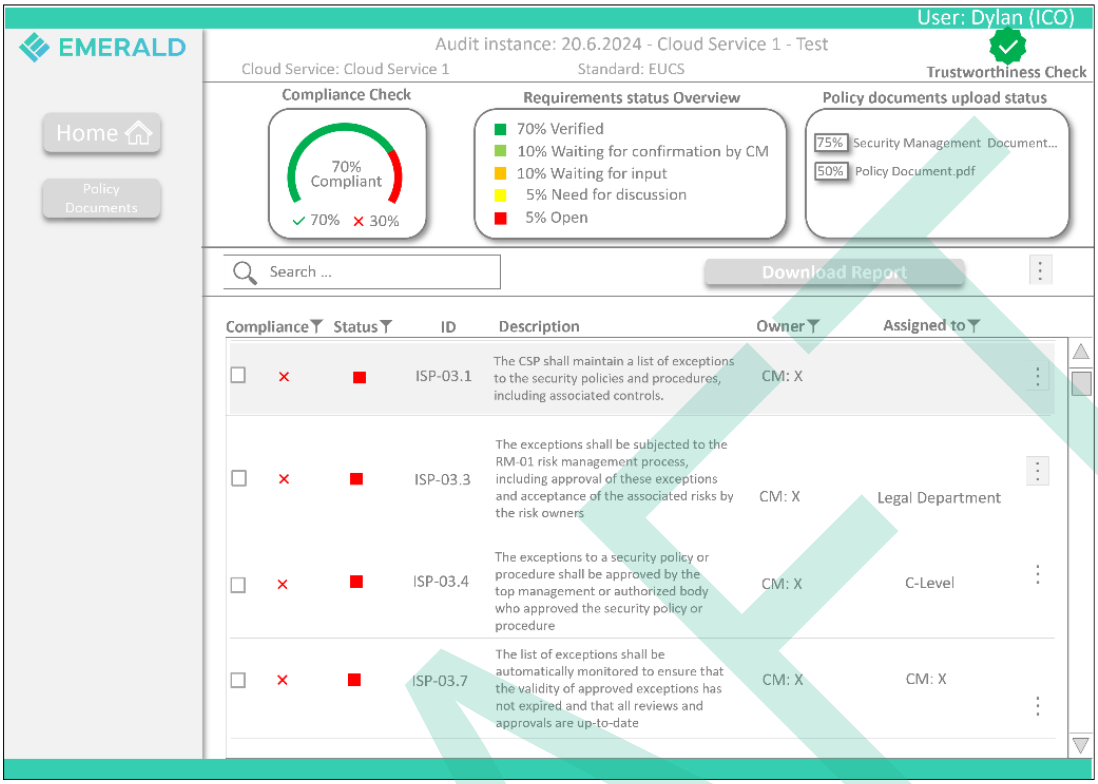

Figure 131. Paper-based Mock-ups – User Journey 2 – Step 1: List of open controls

Figure 132 presents the UI for assigning a control to either an individual person or to a whole department.

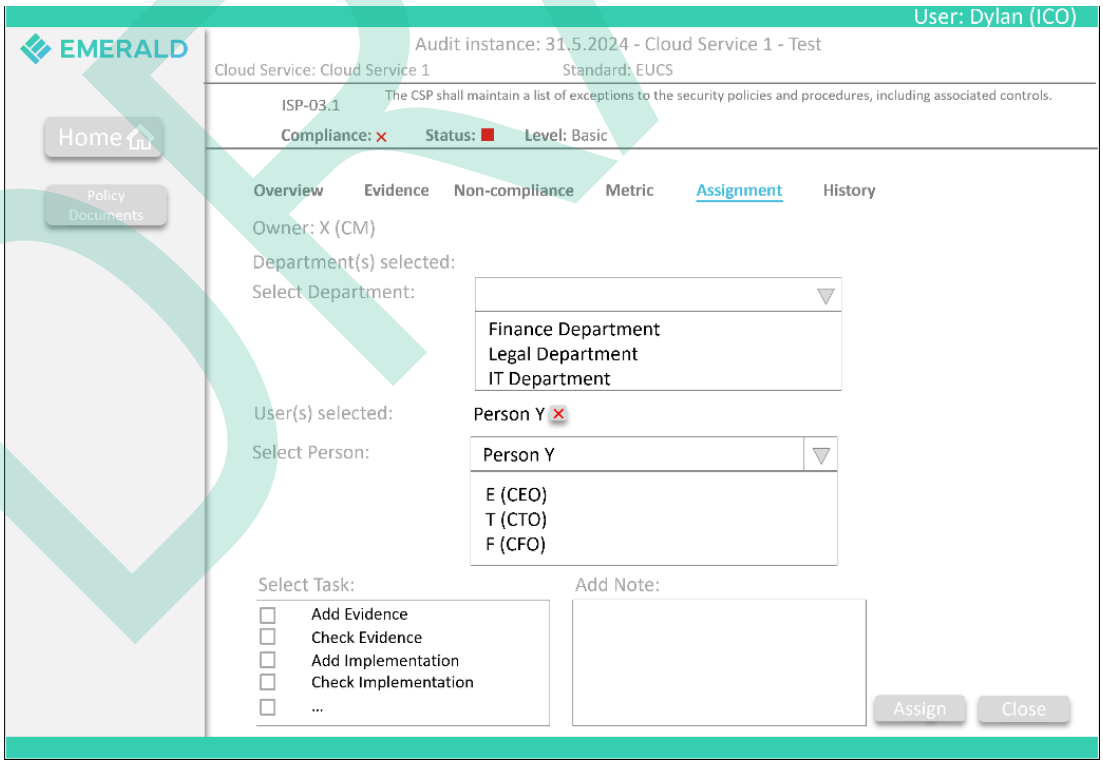

Figure 132. Paper-based Mock-ups – User Journey 2 – Step 2: Assigning control to employee/ departments

Figure 133 presents an example of how the individual workspace looks like. Additionally, it shows the person's assigned number of tasks.

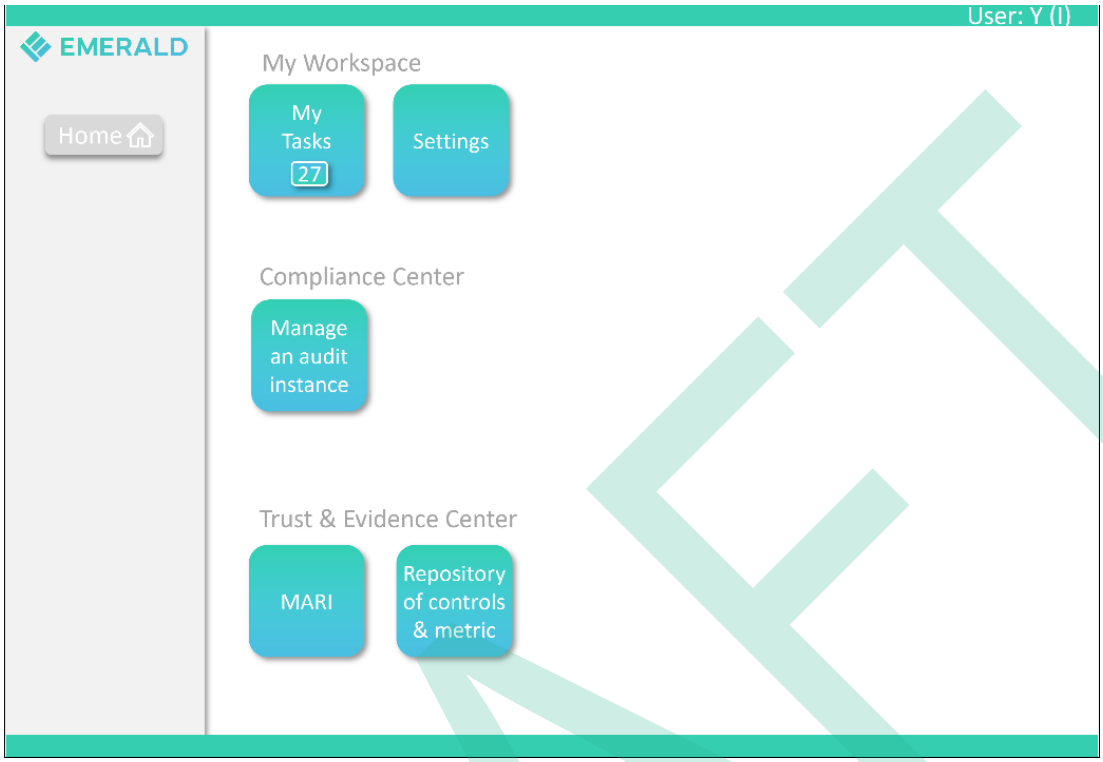

Figure 133. Paper-based Mock-ups – User Journey 2 – Step 3: Personal workspace

10.3 User Journey 3: Charlie – Preparation of an audit by an internal auditor

The scenario for Charlie was divided into five steps as depicted in Figure 134. For each step, first Charlie's task is described and then the interaction with the EMERALD UI.

Step 1:

- **Charlie's Task**: Charlie is an internal auditor at a Cloud Ferro and is responsible for the management of the audit processes against EUCS, including the preparation of the audit. Charlie needs to review all the controls and check if all have their respective evidence assigned to them.
- **Charlie's Interaction with the EMERALD UI:** no interaction is required.

Step 2:

- **Charlie's Task**: Charlie enters the EMERALD UI/UX, looks for the controls related to EUCS high.
- **Charlie's Interaction with the EMERALD UI**: 1) Charlie logs into the EMERALD UI/UX. 2) Charlie selects the components to be audited. 3) Charlie selects the EUCS scheme. 4) Charlie looks for the associated controls.

Step 3:

- **Charlie's Task**: Charlie checks the non-conformities of the associated evidence.
- **Charlie's Interaction with the EMERALD UI**: 5) Charlie clicks on the red flag /icon for the controls that are not compliant.

Step 4:

- **Charlie's Task**: When Charlie discovers a non-compliance, Charlie wants to see which of the metric/assessment result is causing that non-compliance so that they can inform the compliance manager.
- **Charlie's Interaction with the EMERALD UI**: Charlie opens the detailed view on the non-conformities cause: not reaching the threshold, metric not measured (connection lost, etc...), non-trustworthy evidence, etc.

Step 5:

- **Charlie's Task**: Once Charlie has reviewed all the non-compliances they complete an internal report for the compliance manager.
- **Charlie's Interaction with the EMERALD UI**: Charlie exports the summary of the non-conformities (including the detailed information).

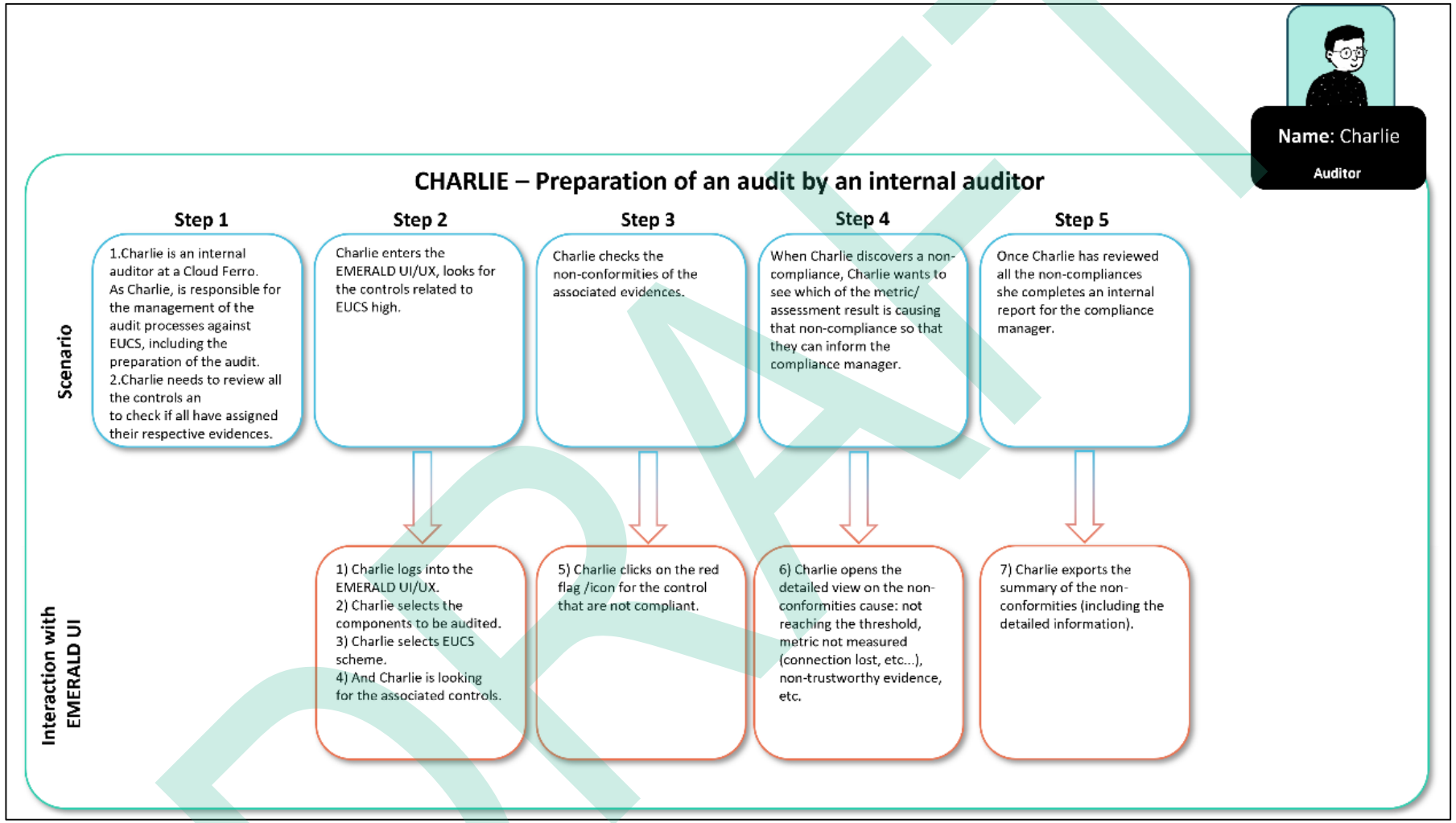

Figure 134. User Journey 3: Charlie – Preparation of an audit by an internal auditor

10.3.1.1.1 Mock-ups: Charlie – Preparation of an audit by an internal auditor

Based on the user journey from Charlie, we have created a set of mock-ups that maps parts of the user journey to the mock-ups. In the case of user journey 3, we have mapped the whole user journey steps 2-5, setting up a new audit scope (Step 2), filtering for non-compliant controls (Step 3), checking the reason for non-compliance (Step 4), and downloading a report (Step 5).

Figure 135 presents the mock-up for setting up a new audit scope in EMERALD.

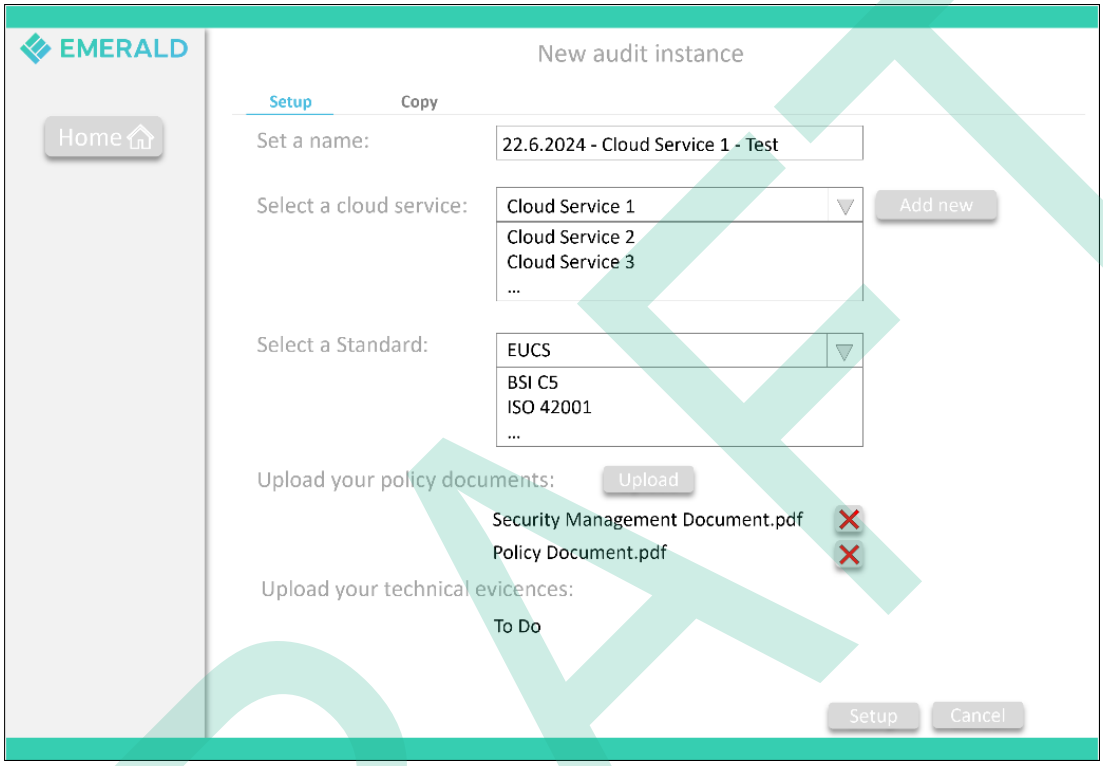

Figure 135. Paper-based Mock-ups – User Journey 3 – Step 2: Setting up a new audit scope

Figure 136 presents the overview of the audit scope including the control list.

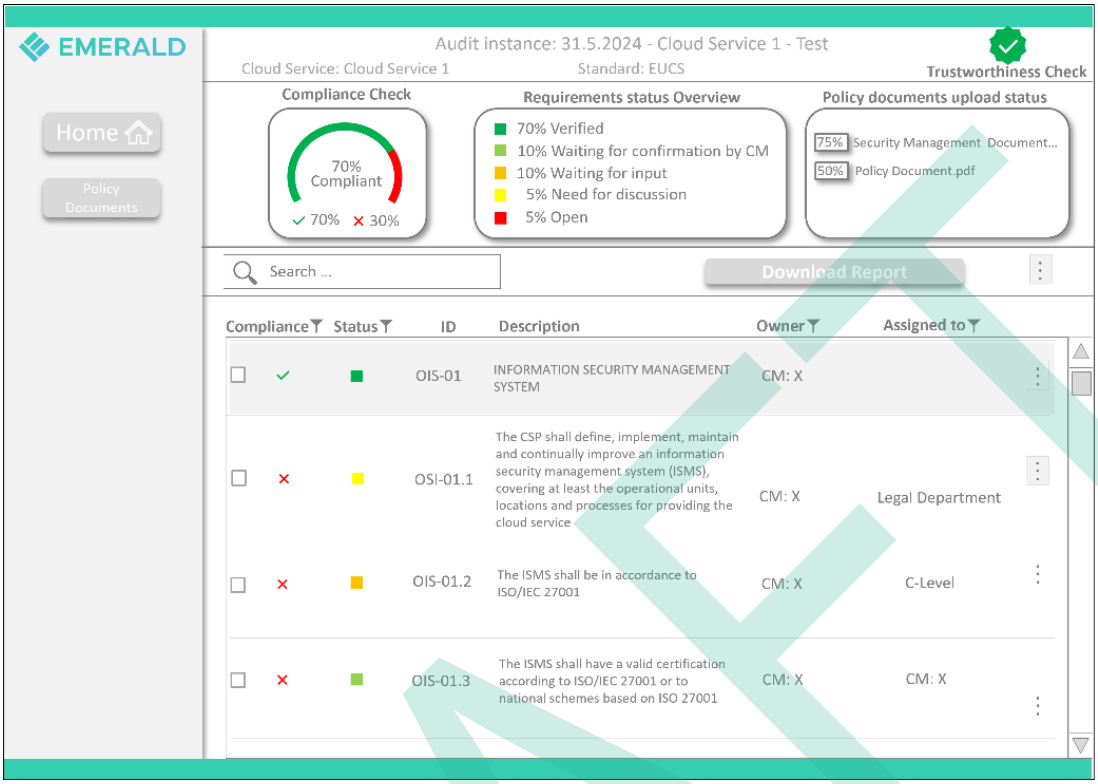

Figure 136. Paper-based Mock-ups – User Journey 3 – Step 2: Audit scope overview

Figure 137 shows how to filter for non-compliant controls in the control list.

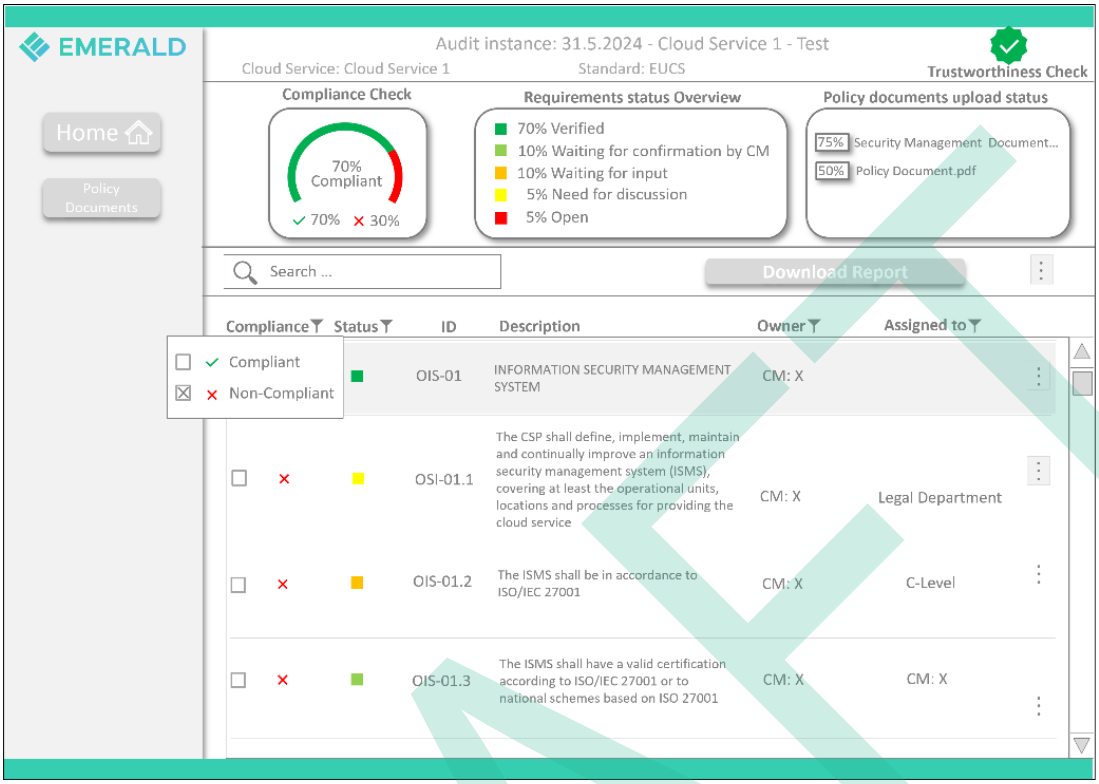

Figure 137. Paper-based Mock-ups – User Journey 3 – Step 3: Filter for non-compliant controls

Figure 138 presents how to quickly check for the reasons of a control marked as non-compliant.

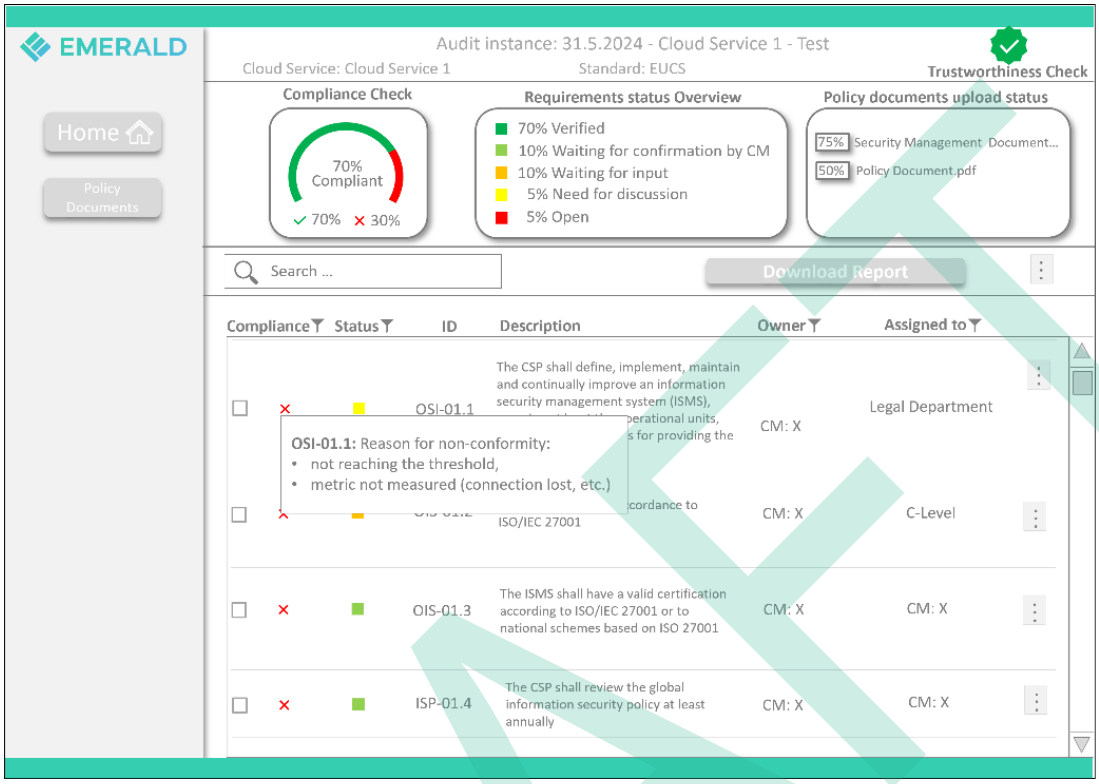

Figure 138. Paper-based Mock-ups – User Journey 3 – Step 4: Check reason of non-compliance

Figure 139 presents more detailed information about why a control is non-compliant.

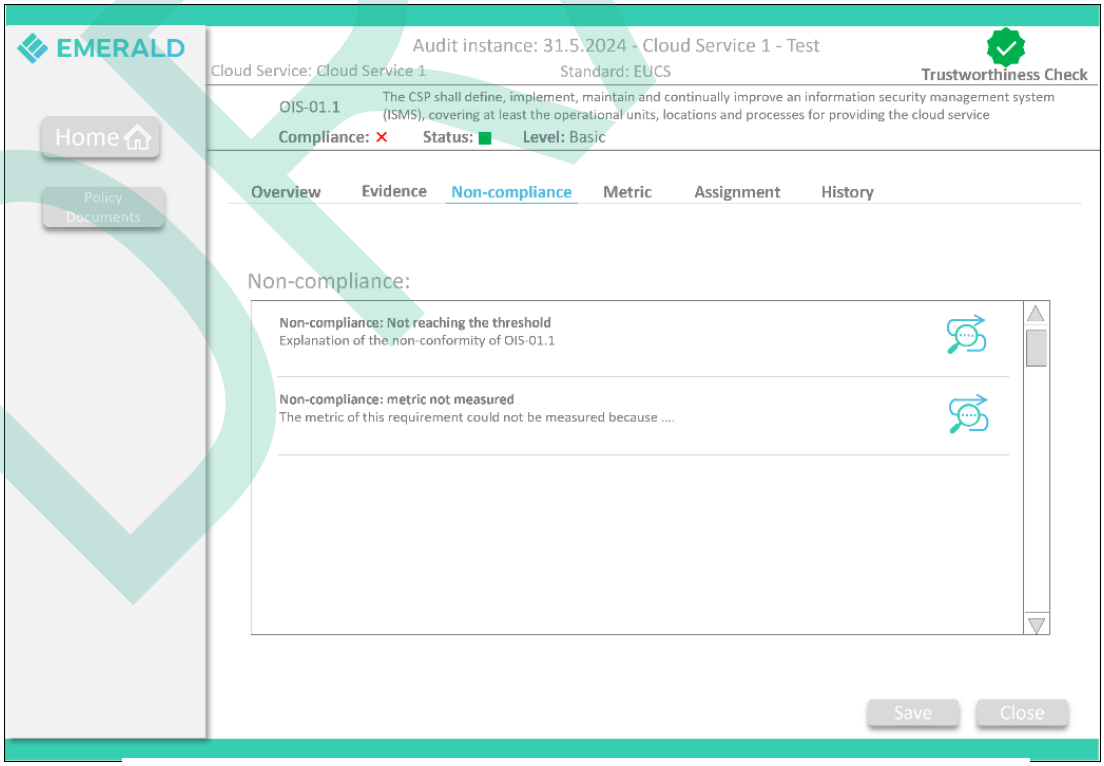

Figure 139. Paper-based Mock-ups – User Journey 3 – Step 4: Information of non-compliance

Figure 140 presents the mock-up of how to download the report about non-compliant controls for a compliance manager.

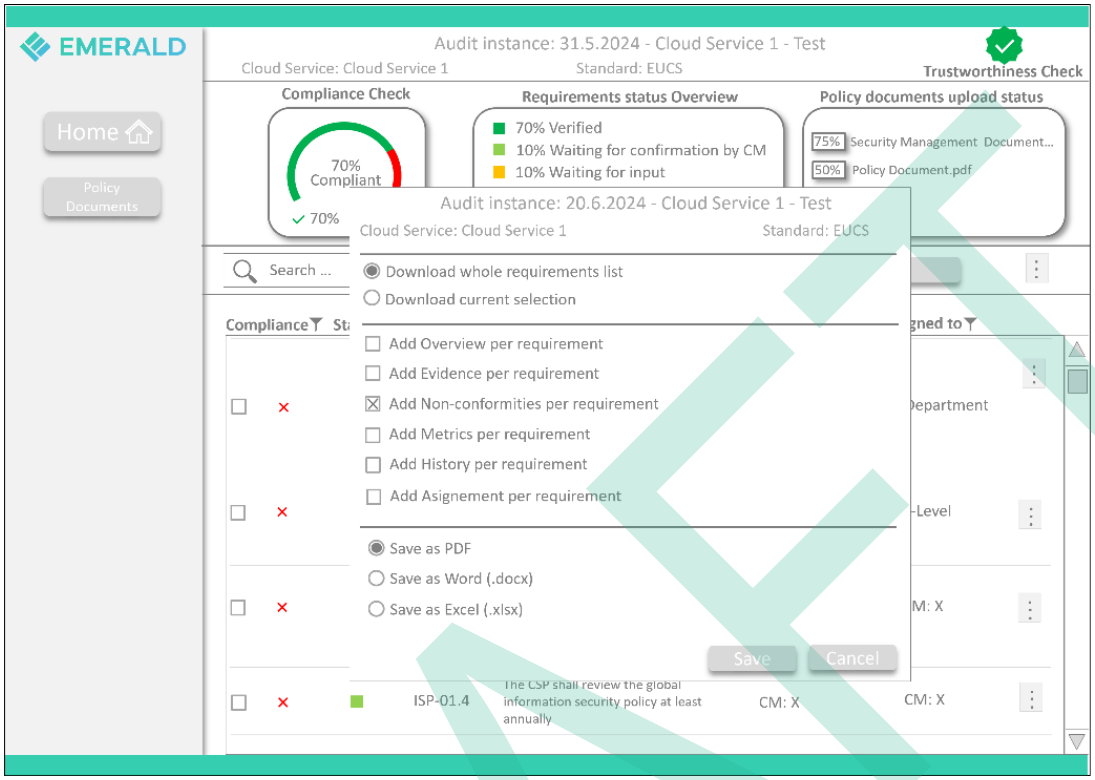

Figure 140. Paper-based Mock-ups – User Journey 3 – Step 5: Download the report