European Commission | Horizon 2020 European Union funding for Research & Innovation

Horizon 2020 Marie Skłodowska-Curie
Research and Innovation Staff Exchange Evaluations (RISE)

AERAS

A CybEr range tRaining platform for medicAl organisations and systems Security

D5.2: AERAS Evaluation Framework and Pilot Set Up Guidelines †

Abstract: This deliverable constitutes the main output of Task 5.2 and describes the building blocks for the AERAS Evaluation phase.

Contractual Date of Delivery	31/07/2024
Actual Date of Delivery	31/08/2024
Deliverable Security Class	Public
Editor	Fulvio Frati (UMIL)
Contributors	Konstantinos Kalais (CUT) Stella Tsichlaki (PAGNI) Nikolas Ioannou (TRID) Dimitrios Dounas (TRID)
Quality Assurance	George Kagadis (UPAT) Evangelos Floros (PAGNI) Konstantinos Papadamou (TRID)

† *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 872735.*

The *AERAS* Consortium

Universita degli Studi di Milano	UMIL	Italy
Technologiko Panepistimio Kyprou	CUT	Cyprus
Sphynx Analytics LTD	STS-CY	Cyprus
AEGIS IT RESEARCH GMBH	AEGIS	Germany
Panepistimiako Geniko Nosokomeio Irakleiou	PAGNI	Greece
Panepistimio Patron	UPAT	Greece
TRID TRINOMIAL TECHNOLOGIES LTD	TRID	Cyprus
Ethical AI Novelties	EAIN	Cyprus
Libra AI Technologies	LIBRA	Cyprus

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Kagadis (UPAT)*
2. *Evangelos Floros (PAGNI)*
3. *Konstantinos Papadamou (TRID)*

Revisions

Version	Date	By	Overview
1.0	31/08/2024	Editor	Final version ready for submission
0.7	30/08/2024	Editor	Reviews received from UPAT, PAGNI, TRID
0.5	15/08/2024	Editor	Version ready for internal revision
0.4	05/08/2024	Editor	Included Section 4
0.3	15/07/2024	Editor	Included Section 3
0.2	01/06/2024	Editor	Included Section 2
0.1	03/05/2024	Editor	First Draft of the table of contents

Executive Summary

Deliverable D5.2 constitutes the main output of Task 5.2 and defines the refined set of KPIs, criteria and methodology to evaluate the AERAS platform. It also provides detailed guidelines and documentation to support the piloting phase, including the ethics approval applications.

The deliverable provides templates for the questionnaires and forms the trainees to be administered to trainees to collect their feedback and acceptance on the AERAS framework. The feedback will then be consolidated and included in the final evaluation report.

Table of Contents

List of Figures

List of Tables

Table of Abbreviations

BSC	Balanced ScoreCards
CIA	Confidentiality, Integrity, Availability
CRSA	Cyber Range Security Assurance
CRST	Cyber Range Simulation and Training
DoA	Description of Action
DDoS	Distributed Denial of Service
KPI	Key Performance Indicator
WP	Work Package

1. Introduction

The goal of the AERAS project is to provide a complete and effective training platform specifically tailored to organizations in the healthcare sector, thus considering all the peculiarity of this critical context.

More precisely, this deliverable describes the outcome of the initial work of Task 5.2, that oversees developing and specifying the evaluation methodology and the associated KPIs that will be used to assess AERAS in the two pilots and beyond them.

Towards this, the team will define appropriate criteria and methodologies that reflect the Key Performance Indicators (KPIs) defined in the project's Description of Action (DoA), and considering the full set of training and functional requirements identified in WP2.

The outcome of the work will be to set the stage for the consolidated reports that will be the base for the final evaluation deliverables D5.5 and D5.6, constituting an analysis of the actual effectiveness and quality of the AERAS platform.

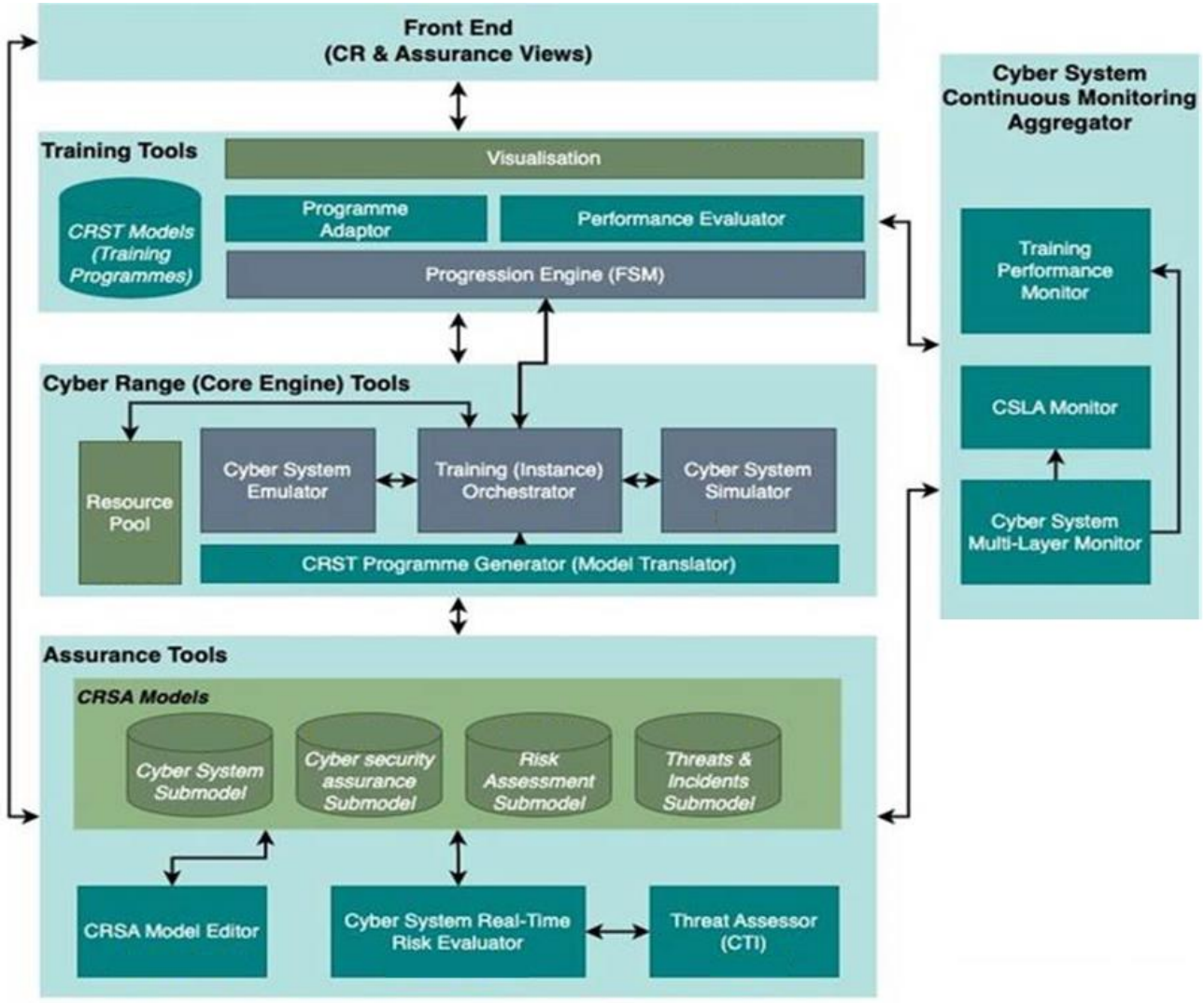

Figure 1: AERAS reference infrastructure.

The work is horizontal with respect to the whole AERAS framework depicted in Figure 1, since all the modules and tools will contribute to the training activities and framework that will be subject of the evaluation work.

1.2 Role of the Deliverable

The role of this deliverable is to provide a clear and effective methodology to evaluate the effectiveness and quality of the training programme and framework provided within the AERAS project.

The deliverable is part of the overall Objective 3 for the aspect related to the monitoring and use of the feedback received from the various component of the framework.

Since the task is horizontal with respect to the other project activities, it will take into consideration all the objectives stated in the project description.

1.3 Relationship to other Deliverables

The Deliverable D5.2 is strictly related with Deliverables D5.5 “AERAS Final Prototype Pilot Validation Report” and D5.6 “Final AERAS Evaluation Report”, setting up the stage for them and defining the reports over which the platform evaluation analysis will be based.

The deliverable is also strictly related to Deliverable D2.1 “Healthcare Pilots & Cyber Range Training Requirements Analysis Report”, since the functional and training requirements defined within WP2 will be evaluated with respect to the actual training activities.

1.4 Structure of the document

The deliverable is structured as follows:

Section 2 provides the building blocks for the evaluation methodology, indicating the needed steps for the system readiness, user familiarization, and pilots’ set-up.

Then, Section 3 constitutes the core of the deliverable providing the template for the User Evaluation questionnaire, Training Requirements Assessment report, and the System Defect Registration form.

Finally, Section 4 describes the structure of the Balanced Scorecard-based consolidated report, and Section 0 draws our conclusions.

2. Definition of the Evaluation Methodology

In this section we define the building block of the evaluation methodology that will be described in detail in the next sections.

In particular, we take into account concepts like system readiness, users' familiarization, and training requirements. These building blocks will be used in the following to build the final balance scorecard to get the final AERAS platform evaluation score.

2.1 System Readiness

The Evaluation and Adaptation checklist provided in Deliverable 4.2 "AERAS Monitoring, Assessment and Adaptation mechanisms – V1" provides a list of phases and tasks that needs to be accomplished to start the training activities. These steps make sure that the AERAS methodology is followed in full and that all the preparatory actions are followed and completed before starting the actual training. Figure 2 graphically depicts the checklist to give us a clear view of the needed steps.

Figure 2: AERAS Evaluation and Adaptation Checklist.

In particular, to achieve the system readiness and start the training, given that the platform is fully functional and operative, Phase 1 and Phase 2 must be executed.

Phase 1 deals with the preparatory work needed to collect data to populate the CRSA and CRST models. As described in D4.2, during Task T1.1 the Threat Assessor tool is run to collect data about the actual threat and vulnerabilities that are present in the hosting environments.

This is of paramount importance to define the cybersecurity baseline of the organization before starting with the training. Then, collected data are fed to the Cyber System Real-Time Risk Evaluator to calculate the overall cybersecurity risk, following the rules described in D4.2.

The completion of Phase 1 tasks allows the execution of Phase 2, where the data are used to fed and populate the CRSA and CRST models. The models are the core object of the AERAS methodology, since they include all the data needed to create and administer the training activities.

As soon Phase 1 and 2 are completed, and the system is declared fully operative by the technical team following the Technical Testing Process described in D5.1, the AERAS platform can be declared “Ready to work” and the training can start.

2.2 User Familiarization

Before being able to start the actual training activities, and to have a successful implementation and evaluation of the pilots, it is important to prepare a familiarization plan, where the trainees will have a first interaction with the AERAS platform, giving them the opportunity to provide fruitful feedback to be exploited in the refinement of the activities and in the Continuous Development strategy of the project.

Initially, the team in the pilots will make a first presentation and demonstration of the platform to a restricted number of the main trainee types. Feedback will be collected concerning the overall approach and user-friendliness, as well as, the learning topics, the defined scenarios so far, and the training modules. Based on this information, we will elaborate better the security goals that will be monitored and the learning path that will be supported.

Thereafter, we will be ready to perform the training to the selected trainees. As part of the readiness check, the platform should be available and functional, and the users able to access it. This involves i) on-line access to the platform through Internet or ii) the local installation of the AERAS platform server and the training in the pilots’ premises.

The exact training activities schedules will be decided by each pilot team during the preparation phase depending on the working duties and organization. Also, there could be more than one training sessions.

Moreover, the provided training material will follow a standardized format to further facilitate the learning process. Templates for the various document types (e.g. lectures, presentations, etc.) have been uploaded in the project SharePoint and will be followed by the trainers for the preparation of the teaching material. Actors engaged in the implementation of pilots, along with their roles and responsibilities are identified in Table 1.

Table 1: Training Team Roles and Responsibilities.

Roles	Responsibilities
Pilot Manager (UMIL, TRID)	- Monitor and maintain pilot execution plan - Ensures that AERAS system is accessible to users (in communication with platform technical support team) - In charge of user familiarization with the platform - Coordinates the re-design of CRSA and CRST models and upgrade of AERAS capabilities between the two pilots implementation against pilot owner specifications
Pilot Owner Moderator (PAGNI/UPAT)	- Organizes the scheduling of training sessions - Instructor of training scenarios - Provides the training scenarios and tracks their progression and results - Evaluates the competence levels gained by the trainees - Sign-off pilot and validate if AERAS meets pilot's requirements
Trainees/Users of different types: - Admin - Managers - Nurses - Doctors	- Connect to AERAS Platform and select the training scenario - Play the selected scenario - Verify results and fill post-training questionnaires

2.3 Pilot Set-up Procedure

With the aim of achieving comparable results and evaluation KPIs, it is important that both pilots provide the trainees with the same training environment, and follow the same preparatory steps. It is important to note that, given the high specificity of the sector where the pilots are involved (healthcare), the evaluation will be strictly dependent on the actual needs and emergencies of the common working activity, and little discrepancies between the two pilots will be considered not relevant for the evaluation itself.

The Pilot Set-up procedure is composed of four steps.

First, the **system readiness** will be executed as described in Section 2.1, that will lead into the population of CRSA models and the definition of training activities within the CRST models. This step will start **at least a month before training** and will be supported by the whole Consortium.

The Pilot Owner Moderator will be responsible of closing the system readiness step after testing the platform. In this phase, the moderator will also recruit trainees among the pilot employees. Following the project DoA, the evaluation should involve a total of 640 hours of training, distributed on average, for each pilot, on 20 participants for 16 hours each (**DoA KPI 15**).

To close the system readiness phase, the moderator will supply the pilot manager with the schedule of participants and the time slots of their training. Furthermore, following **DoA KPI 4**, the selected trainees must belong at least to two different user types (e.g. network manager and doctors).

Second, during the **user familiarization** step, as described in Section 2.2, the pilot owner will instruct the trainees on the use of the platform, via remote or in presence presentation of the platform.

Given the peculiarity of the pilots, since it will be impossible to have all the trainees gathered for the platform presentation, recording of the platform presentation will be allowed. This phase will occur few days before the training start.

It is important to note that a complete and effective user familiarization will be of paramount importance for a good evaluation and understanding of the platform by the trainees, positively affecting the user acceptance value.

Finally, to guarantee the same baseline between the two pilots, the trainees of both PAGNI and UPAT will receive the same identical platform presentation.

At this point, the **training step** can start. The Pilot Owner Moderator will have the task of administer and collect before the training the AERAS Consent Form and Information Sheet, that will be conserved by the pilots themselves.

Third, at the end of each training session, the moderator can start the **individual evaluation step** administering the user acceptance, the Training Requirement Assessment form, and the System Defects Registration forms, as described in Section 3.1, Section 3.2, and Section 3.3. During this phase, it is important also that the moderator take note of verbal comments that can be included in D5.5 “AERAS final prototype pilot validation report”. All the comments and forms will be compiled anonymously and no reference to the trainees will be included in them.

Finally, at the end of the previous phase, the moderator will enter in the **reports consolidation** step to complete the training session and prepare the consolidated reports (See Section 3), that will be handled to the Pilot owner. The consolidated reports will be used as base for the D5.5 and D5.6 “Final AERAS evaluation report”.

All the training should end at least at M65, to allow the submission on time of the final WP5 deliverables.

2.4 Functional Requirements

Deliverable D2.1, through interview and focus groups, the team defined the main high-level functional requirements that the platform should satisfy.

In the evaluation methodology depicted in the next sections, we will take them into consideration defining in which measure they are satisfied. It is important to note as functional requirements we consider “training requirements”, specific training needs the AERAS platform should support.

Table 2: Functional Requirements list.

Req. ID	Description	Priority	Use Case
FR_01	Social Engineering: Phishing	**MUST**	**Personnel: IT-experts and non-IT experts** The trainee receives a phishing email that prompts him/her to click on a link to change a password because it is expired. Assess the user's behavior.
FR_02	Social Engineering: Spear Phishing	**MUST**	**Personnel:** **IT-expert** Non-IT personnel reports being a victim of (spear) phishing, and that incident concludes in the user sharing credentials for access to an organization's system; Assess how the IT will respond to the incident. **Non-IT experts** The trainee receives a spear phishing email with the signature of a member of the IT staff with an attachment and asks the user to download and run the file to update a known user software on their device; Assess the user's behavior.
FR_03	Sharing patient's information	**MUST**	**Personnel: non-IT experts** Best practices for secure sharing patient's information (inside and outside of the organization) must be made available for consultation.
FR_04	Data Breach and GDPR compliance	**MUST**	**Personnel: IT-experts and non-IT experts** There is a confirmed incident of data breach. Assess the actions of the personnel in regard to compliance with GDPR.
FR_05	DDoS attacks	**MUST**	**Personnel: IT-experts** The personnel cannot access the services and data systems. The trainee, provided with the network logs, must identify a DDoS attack occurring and respond to the threat; Assess the trainee's performance.
FR_06	Malware	**MUST**	**Personnel:** **IT-experts** - Configuration of the central firewall and endpoint antivirus for the organization system; Assess the performance of the trainee. - Someone reports malware detection on their machine and asks for the help of the IT staff; Assess after-call actions of the IT. **Non-IT experts** The antivirus on the trainee machine detects malware while scanning; Assess the trainee behavior.
FR_07	Ransomware attack	**MUST**	**Personnel:** **IT-experts** The trainee is aware of a ransomware attack on the organization systems; Assess the trainee actions to handle the incident. **Non-IT experts** The screen of the machine is locked, there is a message informing of a ransomware attack and demanding a ransom to unlock the

			screen, threatening the organization to disrupt the operations and breach private data. Assess the user's behavior and awareness of ransomware attacks.
FR_08	System Failure	**MUST**	**Personnel: IT-experts & non-IT experts** The trainee faces an unexpected system failure. He/she has to identify the reasons and the criticality of the incident. Assess the user's behavior.
FR_09	Web navigation	**MUST**	**Personnel: Non-IT experts** The trainee, while navigating the web, will be faced with a request for downloading an application/file or system update. Assess how the user will comply with security policies.
FR_10	Software Updates	**MUST**	**Personnel: Non-IT experts** The trainee, while interacting with the system, is notified of a software update. Assess the trainee's behavior.
FR_11	Database management and security updates	**MUST**	**Personnel: IT experts:** There was an attempt to access and modify the organization's database with the patient's data (i.e., SQL injection). Assess the trainee's investigation of the incident and the security measurements he/she takes to prevent it from happening again.
FR_12	Cyber Risks in relation to the physical presence of external actor/device	**MUST**	**Personnel: IT-experts** A non-institutional device is connected to the organization's network and there is a number of unsuccessful trials to access the information system. Assess the trainee behavior.
FR_13	Firewall and antivirus	**MUST**	**Personnel: IT-experts** Train the IT-experts for configurating and managing the Firewall, and end point antivirus to the organization equipment. Assess the trainee performance.

FR_14	CIA	**MUST**	**Personnel: IT-experts**
			CIA triad is essential for an organization's security infrastructure to set the goals and objectives for every security program.
			• Confidentiality means that only authorized users and processes should be able to access or modify data.
			• Integrity means that data can be trusted. Prevent unauthorized parties to alter the data.
			  o Understand the fact that Cryptography is essential to ensure confidentiality and integrity.
			• Availability means that Authorized parties can access and use data anytime.
			  o Understand that Denial of service attacks are attempts to block availability.

			Assess the trainee understanding of the CIA properties.
FR_15	Password management	**MUST**	**Personnel:** **Non-IT personnel** Safeguarding passwords, create strong passwords. Assess the trainee performance. **IT-experts:** Procedures for creating, changing, and safeguarding passwords. Implement strong passwords and multi-factor authentication. Assess the trainee performance.
FR_16	VPN handling	**SHOULD**	**Personnel: IT experts** The trainee will understand the benefits and learn about the best practices for using a VPN connection to help secure their organization network. VPN Configuration. Assess the trainee performance.
FR_17	Synthetic data	**MUST**	Data used in training activities must be synthetic data. Furthermore, the synthetic data must be realistic.
FR_18	Platform functionality and responsiveness	**SHOULD**	The AERAS platform should be functional and responsive.
FR_19	User guidance through the AERAS platform	**SHOULD**	Design a user manual for the users of AERAS cyber range training platform. The manual needs to be user-friendly, and easy to follow for both IT experts and non-IT personnel.
FR_20	User interface	**SHOULD**	The trainee should be faced with a set-up that replicates as much as possible the real working environment
FR_21	Trainers	**SHOULD**	Trainers should be able to assess trainees progresses and activities
FR_22	Continuous training	**SHOULD**	The trainee should be able to repeat the same training activity periodically.
FR_23	Training documentation	**SHOULD**	Documentation specific for the single training activity (whitepaper, manual, slides, etc.) should be made available to the trainee

3. Pilot Checklist

During and post pilot execution, trainee will be asked to give their feedback about the AERAS framework. This will be used to get a qualitative and quantitative evaluation of the effectiveness and usability of the tool.

In particular, the three aspects that will be examined will be:

- User acceptance, via a specific User Evaluation questionnaire.
- Training requirements assessment report, filled by the pilot moderators collecting post-training user's comments.
- System defects form, filled by the users indicating specific defects that the team needs to solve to improve the platform quality.

In the following sections, we provide templates of the questionnaires that will be administered. It is important to note that the questionnaire can be improved if some changes are overseen after the conclusion of the development phase.

3.1 User Evaluation Questionnaire

This document will be administered to trainees upon completion of pilot training sessions. The Pilot Owner Moderator will then aggregate feedback from the trainees/users and results will be handed over to the pilot manager.

Figure 3: User Evaluation Questionnaire high level document flow.

The document will be organized as a common questionnaire (depicted in Table 3) that will give to the trainees the possibility to express their acceptance of the platform as a whole. Grades will be given following a 5-level Likert scale [1]. It should be noted here that the choice of "questions asked" – parameters assessed has taken into consideration specific software Quality Models [2] (reference to ISO 9126:2001[1] and ISO 25010:2011[2]).

1- Strongly Disagree
2- Disagree
3- Neither agree nor Disagree
4- Agree
5- Strongly Agree

[1] http://www.sqa.net/iso9126.html
[2] https://www.iso.org/standard/35733.html

Table 3: User acceptance questionnaire (preliminary version).

1. The AREAS Platform is easily accessible					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				
Comments					
2. You can easily navigate in THREAT-ARREST environment (menu, links, documents)					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				
Comments					
3. The explanation given are complete and allow me to use the Platform without problems					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				
Comments					
4. The platform has been an effective tool to reach the defined training requirement					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				
Comments					
5. The platform interface is complete and easy to use					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				

Comments					
6. Set-up time for learning activities (from the time the activity is request to the time the environment is accessible) are adequate					
	1	2	3	4	5
	1- Strongly Disagree 2- Disagree 3- Neither agree nor Disagree 4- Agree 5- Strongly Agree				
Comments					

3.2 Training Requirements Assessment Report

The role of the Training Requirement Assessment Report is to assess whether the training activities, proposed by the team to the trainees, satisfies, or not, the functional requirement stated in Deliverable D2.1.

This document will be prepared by the Pilot Owner Moderator, given the feedback from the system evaluation by the trainees, and will be handed over to Pilot Manager for his consideration and action, following the flow indicated in Figure 4.

Figure 4: Training Requirement Assessment Report High level document flow.

The template proposed in Table 4 proposes all the training requirements with the schema to indicate whether the requirement has been satisfied or not. The Pilot Owner moderator will extract, for each training activity, the specific requirements and propose them to the trainees after the execution of the activities. Specific requirements can be related to more than one training activities. Specific details on the requirements can be found in Table 2 and in Deliverable D2.1.

The integrated documents, with all the feedback collected, will give an idea of the completeness of the training programmes proposed by the team for the evaluation phase.

Table 4: Pilot Training Requirement satisfaction template.

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_01	Social Engineering: Phishing				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_02	Social Engineering: Spear Phishing				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_03	Sharing patient's information				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_04	Data Breach and GDPR compliance				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_05	DDoS attacks				

Comment	

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_06	Malware				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_07	Ransomware attack				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_08	System Failure				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_09	Web navigation				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No

FR_10	Software Updates				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_11	Database management and security updates				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_12	Cyber Risks in relation to the physical presence of external actor/device				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_13	Firewall and antivirus				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_14	CIA (Confidentiality, Integrity, Availability)				
Comment					

Requirement ID	Requirement Description	Criticality Level	Result

		Yes	No	Yes	No
FR_15	Password management				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_16	VPN handling				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_17	Synthetic data				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_18	Platform functionality and responsiveness				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_19	User guidance through the AERAS platform				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_20	User interface				
Comment					

Requirement ID	Requirement Description	Criticality Level		Result	
		Yes	No	Yes	No
FR_23	Training documentation				
Comment					

3.3 System Defect Registration Report

This report will record critical, major and minor defects (bugs, crashes, events) of the final AERAS platform while on operation. Preliminary recordings of observations will be drafted by trainees/users following testing.

Aggregated remarks will be included in a consolidated report of system defects handed over to pilot manager by pilot owner moderator, following the flow in Figure 5.

Figure 5: System Defect Registration document High level flow.

As indicated in Figure 5, the defect form will be administered to the trainees before the training activities. In this way, they can take note of all the defects that occurred during the execution.

Then, all the reports will be collected by the Pilot Owner Moderator, that will integrate all the single contribution in a consolidated defect report to deliver to Pilot Manager. The report will be taken in consideration in future iteration of the development process.

Document for registration of observations by trainee/user per test/session will have the following format, depicted in the following Table 5.

Table 5: Defect report template delivered to Trainees.

Date	**Trainee**	**Pilot**	**Training Activity**
<dd/mm/yyyy>	<name/role>	<UPAT/PAGNI>	<name of activity>
Defect Observation			
#	**Description**	**Comment**	

In turn, Table 6 shows the template for the consolidated report, created by the Pilot Owner Moderator taking into consideration all the collected Trainee's defect form. In this, all the defects are organized by training activity and ordered by severity.

The severity will be categorized with respect to the following criteria:

- **Critical**: An unexpected incident that terminates training procedure.
- **Major**: An unexpected incident that leads to erroneous or partial training process.
- **Minor**: An unexpected incident that has insignificant impact on the training process (e.g. small delay).

Table 6: Consolidated Defects Report form templated for Pilot Owner Moderators.

Date of training	**Pilot Owner Moderator**	**Pilot**	**No. training session performed**
<dd/mm/yyyy>	<name/role>	<UPAT/PAGNI>	
Consolidated Defect Report			
No.	**Training Activity**	**Description**	**Severity**
			<Critical/Major/Minor

4. Consolidated Pilots Report

The Consolidated Pilots Report, reported in Figure 6, has been defined aggregating significative measure that could give a precise view of the effectiveness and overall quality level of the AERAS platform.

The report is based on the Balance ScoreCard (BSC) approach [3] and elaborate four evaluation level:

- Level 4: High-level evaluation of the platform taking into consideration significant KPIs defined in AERAS Description of Activities (DoA).
- Level 3: Based on feedback from Trainees and Pilot owner, the level of satisfaction of the training activities is evaluated.
- Level 2: the quality of the Learning activities is evaluated using as measure the average grades received by trainees after executing learning activities.
- Level 1: technical aspects, like set-up times, functional capabilities and number of detected defects are considered to evaluate the overall technical quality of the platform.

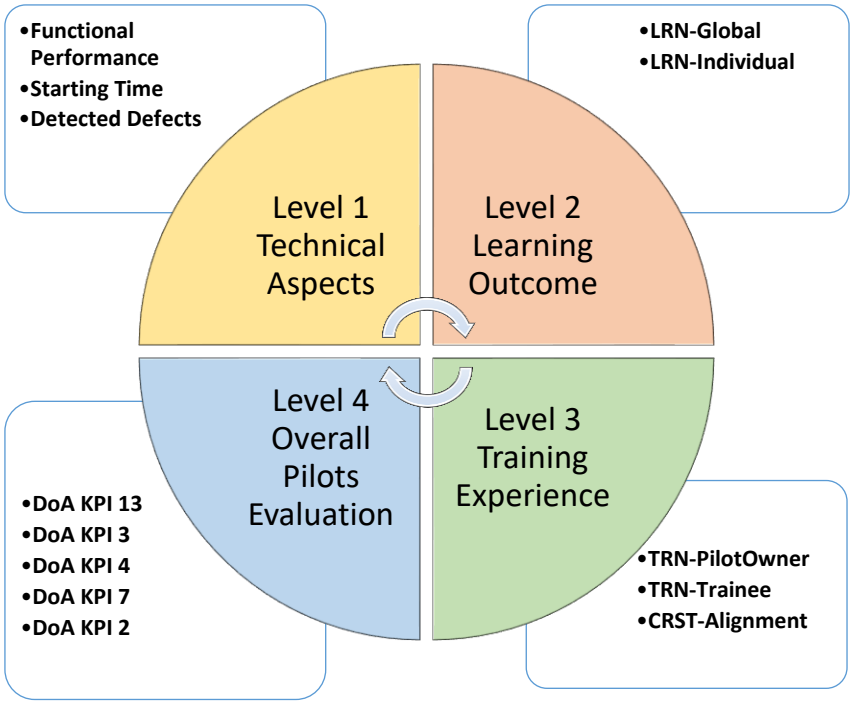

Figure 6: Consolidated Report diagram.

The KPIs described inTable 7 can be updated if the ongoing development of the platform highlight different aspects that can better measure the overall quality. The final table will be then reported in D5.6 “Final AERAS evaluation report”.

The table reports the target value that should be accomplished to declare that the KPI has been satisfied. Target value can be numerical, as for example level 4.1, or textual, like for instance level 4.2.

In case of textual evaluation, the following threshold are considered:

- *Not started*: 0% of considered aspects have been implemented.
- *In progress*: less than 50% of considered aspects have been implemented.
- *Partially*: a level between 50% and 80% of the aspects have been implemented.
- *Fully*: more than 80% of the considered aspects have been implemented.

Table 7: Consolidated Pilots Report (preliminary format).

Level	KPI-Metric	Definition	Measure Method	Target Value
4	**Overall Pilots Evaluation**			
4.1	DoA KPI 13	Delivery of an integrated cyber range training platform, with capabilities described in Objectives 1-4, at TRL7	Based on D5.4, D4.3, D4.4	Fully*
4.2	DoA KPI 3	Deliver at least 4 CSLA templates to cover the basic properties of confidentiality, integrity, availability and privacy, which can be instantiated to support the pilots;	Based on D3.3	Fully*
4.3	DoA KPI 4	Deliver at least 4 CRST programmes to cover the two pilots and two different user types for each of those.	Based on D3.3, D5.5	Fully*
4.4	DoA KPI 7	Delivery of the monitoring and adaptation mechanisms of CRSA models and associated Cyber Range programmes;	Based on D4.2 and D4.4	Fully*
4.5	DoA KPI 2	Develop at least 10 model (fragments) to cover threats (at least 5) and security mechanisms (at least 3 per threat) for at least 4 critical properties (confidentiality, integrity, availability, privacy);	Based on D3.3 and final CRSA/CRST models delivered	Fully*
3	**Training Experience**			
3.1	TRN-PilotOwner	Organizational (Pilot Owner) overall evaluation/satisfaction	Based on D5.3, D5.5	Fully*
3.2	TRN-Trainee	Overall User (Pilot Trainees) Quality of Training Experience – overall evaluation/satisfaction	Based on Trainees Evaluation reports	>=4
3.3	CRST-Alignment	Level of satisfaction related to stated learning requirements	Based on Pilot Training Requirement	Fully*

			satisfaction	
2	**Learning Outcome**			
2.1	LRN-Global	Aggregated training scores per Pilot	Training scores recorded in the AERAS Framework	At least 80% of total score
2.2	LRN-Individual	Individual training score of all trainees, independently from the organization	Training scores recorded in the AERAS Framework	At least 80% of the total score
1	**Technical Aspects**			
1.1	Functional Performance	Actual level of Functional Capabilities	Based on D5.3, D5.5	Fully*
1.2	Starting Time	Time needed to start-up learning activities	Based on question 6) of User Acceptance questionnaire	>= 4
1.3	Detected Defects	No. defects detected by users during the execution of training activities	Based on Consolidated Defects Report	Max 1 major per training activity

5. Conclusions

This deliverable presents the building blocks for the preparation of the final AERAS platform evaluation reports. The deliverable contains the template for the User Acceptance Evaluation Questionnaire, the Training Requirement Assessment, and the System Defects Registration reports.

The report will be administered by the Pilot Owner Moderator to the trainees to collect their feedback on the platform and the training activities and will be consolidated in pilot-specific report to be included in final Deliverables D5.5 and D5.6.

Furthermore, the deliverable defines a Balanced ScoreCard-based report to have a clear view of representative KPIs used to evaluate the effectiveness of the Platform. The results of this report will be examined in Deliverable D5.6.

Finally, in Section 2 the deliverable also set the stage for the training session to be organized at pilots' site. It is important that the preparation of the training, and the training itself, will be conducted in a comparable way for both pilots, to be able to aggregate results coming from trainees. Given the criticality of the two pilots (hospitals), the evaluation phase will be valid even if small deviations from the plan will occur, like for instance the unavailability of some employees to participate to the training and/or the user familiarization.

References

[1] A. Joshi, S. Kale, S. Chandel and D. Pal, “Likert Scale: Explored and Explained,” *British Journal of Applied Science & Technology,* vol. 7, no. 4, pp. 396-403, 2015.

[2] J. Estdale and E. Georgiadou, “Applying the ISO/IEC 25010 Quality Models to Software Product,” in *Software and Services Process Improvement. EuroSPI 2018. Communications in Computer and Information Science, vol 896*, Spinger Charm, 2018, p. 492–503.

[3] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson, “Performance Measurement Guide for Information Security rev. 1,” National Institute of Standards and Technology, 2008.