

**Horizon 2020 Marie Skłodowska-Curie**

**Research and Innovation Staff Exchange Evaluations (RISE)**



**A CybEr range tRaining platform for medicAl organisations and systems Security**

**D4.2: AERAS Monitoring, Assessment and Adaptation mechanisms – V1** [[1]](#footnote-2)†

**Abstract**: This deliverable constitutes the main output of Task 4.2 and describes the Evaluation and Adaptation methodology, that involves most of the tools and procedures of the AERAS framework and provides to trainers and managers of a effective techniques to adapt training programmes to the update cybersecurity landscape.

|  |  |
| --- | --- |
| Contractual Date of Delivery | 31/05/2024 |
| Actual Date of Delivery | 31/05/2024 |
| Deliverable Security Class | Public |
| Editor | Fulvio Frati (UMIL) |
| Contributors | Fulvio Frati (UMIL)  Nikos Salamanos (CUT)  Pantelitsa Leonidou (CUT)  Costas Iordanou (CUT) |
| Quality Assurance | XXXX (UPAT)  XXXX (PAGNI) |

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 |
| Trinomial Technologies LTD | TRID | Cyprus |
| Ethical AI Novelties | EAIN | Cyprus |
| Libra AI Technologies | LIBRA | Cyprus |

*Document Revisions & Quality Assurance*

**Internal Reviewers**

1. *XXXX (UPAT)*
2. *XXXX (PAGNI)*

**Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Overview** |
| 1.0 |  |  |  |
| 0.7 |  |  |  |
| 0.5 | 05/05/2024 | Editor | Version for internal review |
| 0.4 | 28/04/2024 | Editor | Final editing |
| 0.3 | 14/04/2024 | Authors | Included Introduction and conclusions |
| 0.2 | 14/03/2024 | Authors | Inserted section 2 and checklist section |
| 0.1 | 15/02/2024 | Editor | First Draft of the table of contents |

*Executive Summary*

Deliverable 4.2 constitutes the main output of Task 4.2 and describes the Evaluation and Adaptation methodology, that involves most of the tools and procedures of the AERAS framework and provides to trainers and managers of a effective techniques to adapt training programmes to the update cybersecurity landscape.

In the deliverable, the team describes and details the Evaluation and Adaptation checklist and the relation and communication flows among the actors involved in the process.

The described methodology determines one of the key-points of the AERAS framework, that use the improvement of the adopting organization cybersecurity landscape as a measure of the administered training programmes effectiveness.

*Table of Contents*

[1. Introduction 8](#_Toc165636588)

[1.2 Role of the Deliverable 9](#_Toc165636589)

[1.3 Relationship to other Deliverables 9](#_Toc165636590)

[1.4 Structure of the document 9](#_Toc165636591)

[2. Evaluation and Adaptation Checklist 10](#_Toc165636592)

[3. Phase 1: Pre-Training Phase 12](#_Toc165636593)

[1.1 Task 1.1: Pre-training security and risk evaluation (tool) 12](#_Toc165636595)

[1.2 Task 1.2: Training needs analysis (procedure) 14](#_Toc165636596)

[4. Phase 2: Models Population 16](#_Toc165636597)

[2.1 Task 2.1: CRSA Models population (procedure) 16](#_Toc165636599)

[2.2 Task 2.2: CRST Models population (procedure) 16](#_Toc165636600)

[5. Phase 3: Training 18](#_Toc165636601)

[3.1 Task 3.1: Real-time assessment of trainee performances (tool) 18](#_Toc165636603)

[6. Phase 4: Post-Training 19](#_Toc165636604)

[4.1 Task 4.1: Post-training security and risk evaluation (tool) 19](#_Toc165636606)

[4.2 Task 4.2: Production of aggregate data on trainees' activities 19](#_Toc165636607)

[7. Phase 5: Evaluation & Adaptation 21](#_Toc165636608)

[5.1 Task 5.1: Pre- and Post-training security and risk comparison (tool) 21](#_Toc165636610)

[5.2 Task 5.2: Adaptation Analysis of training activities (tool) 22](#_Toc165636611)

[5.3 Task 5.3: Alerts on training adaptation needs 23](#_Toc165636612)

[8. Conclusions 25](#_Toc165636613)

[9. References 26](#_Toc165636614)

*List of Figures*

Figure 1: AERAS reference infrastructure. 8

Figure 2: AERAS Evaluation and Adaptation Checklist. 10

Figure 3: AERAS procedures implementing Task 1.1 12

Figure 4: CVSS metrics composition [5]. 13

Figure 5: Risk evaluation data flow. 14

Figure 6: Kolb's cycle stages of learning. 15

Figure 7: CRSA Submodels. 16

Figure 8: CRST Programme Generator module. 17

Figure 9: Performance Evaluator and Progression Engine. 18

Figure 10: Progression Engine expected communication flows. 18

Figure 11: Post-training risk evaluation flow. 19

Figure 12: Performance Evaluator tool data flow. 20

Figure 13: Training Performance Monitor tool. 21

Figure 14: : Training Performance Monitor expected communication flow. 22

Figure 15: Programme Adaptor tool. 22

Figure 16: Programme Adaptor expected communication flow. 23

*Table of Abbreviations*

|  |  |
| --- | --- |
| **CRSA** | Cyber Range Security Assurance |
| **CRST** | Cyber Range Simulation and Training |
| **CSLA** | Cybersecurity Service Level Agreement |
| **CVSS** | Common Vulnerability Scoring System |
| **DDOS** | Distributed Denials-of-Service |
| **FSM** | Finite State Machine |
| **NIST** | National Institute of Standards and Technology |
| **NVD** | National Vulnerability Database |
| **WP** | Work Package |
|  |  |

# Introduction

One of the strongest point of the AERAS approach is the availability of tools and procedure that allows a continuous assessment of the adopting organizations cybersecurity landscape and related risk. Furthermore, the project improved the expected training programme effectiveness including a specific methodology to adapt the training activities with respect to updated cybersecurity threads and vulnerabilities, and the intrinsic response of trainees to the activities themselves.

The added value of the AERAS framework, in fact, is to evaluate the effectiveness of the training activities evaluating the overall improvement of the risk level of the organization. Going more in details, the risk level of the organization is evaluated before, during and after the execution of the training programme, directly correlating an improvement (or a deterioration) of the risk level with the effectiveness of the training programme. The rationale behind it is that more the organization improve its cybersecurity landscape, the more effective the training programme has been for the organization itself.

The adaptation and evaluation methodologies is described in this deliverable in term of a five-step checklist. Each step is composed of task that drive the trainers and manager in the definition and execution of the procedure. The checklist is connected to most of the AERAS tools and procedures (Figure 1) and involves the whole lifecycle of the framework.

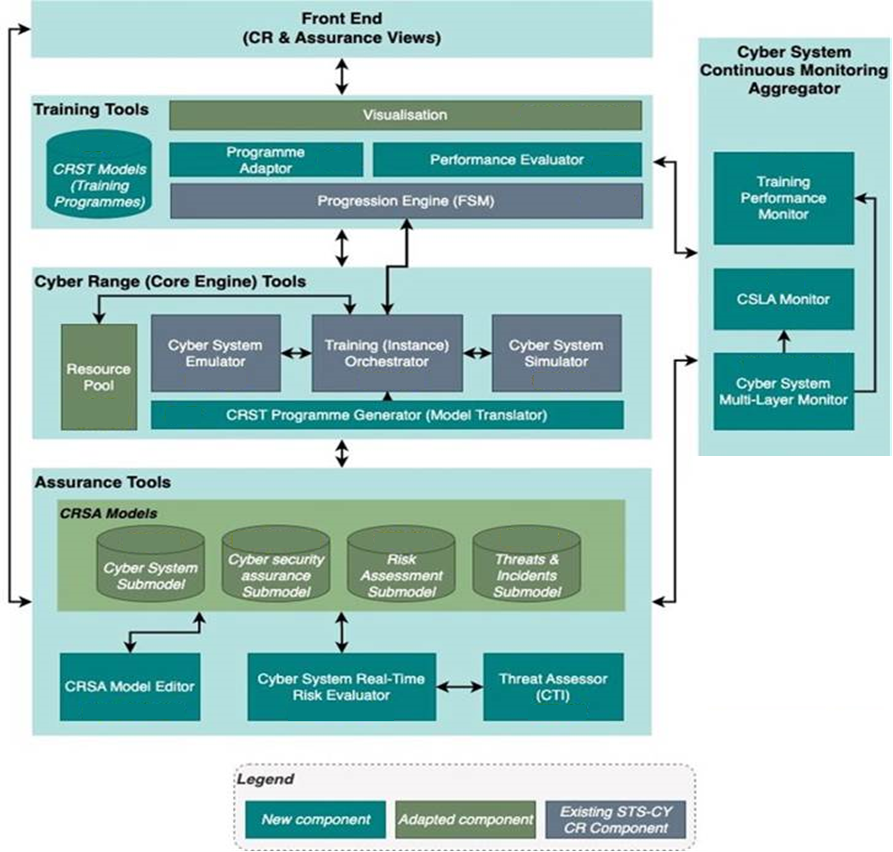


Figure 1: AERAS reference infrastructure.

## Role of the Deliverable

The role of this deliverable is to provide a clear and effective methodology in order to implement the adaptation and evaluation technique of the training programme provided within the AERAS framework.

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.

**Objective 3:** *Develop mechanisms to support the adaptation of cyber range simulation and training programmes, via feedback received from multiple sources, including multi-layer system, trainee and programme performance monitoring, and CSLAs monitoring.*

The deliverable contributes also to Objective 2, that requires a mechanism for the continuous monitoring of the cyber systems and the trainees.

***Objective 2:*** *Develop novel hybrid cyber security risk analysis models, which combine traditional static cyber security risk analysis principles and standards with continuous risk estimates. These estimates are informed from simulation and the continuous real-time multi-layer monitoring of cyber-systems and trainees.*

## Relationship to other Deliverables

The Deliverable 4.2 is strictly related with the deliverables that are part of WP4 and WP3.

In particular, the connection with D4.1 is strict in term of description of the tools and modules that compose the cyber range infrastructure and that are included in the Phase 3 of the checklist described in Section 2.

With respect to WP3, D3.1 is connected with the current deliverable in the work related, in particular, with Phase 2, where the CRSA and CRST models are populated, and Phase 1, where the data will be collected.

## Structure of the document

The deliverable is structured as follows.

Section 2 provide a description of the Evaluation and Adaptation checklist that drive the trainers and managers in the preparation and execution of the methodology.

Sections from 3 to 7 describes the five phases of the methodologies in details, specifying the involved tools and procedures and describing the underlying tasks.

Finally, Section 8 draws our conclusions.

# Evaluation and Adaptation Checklist

The Evaluation of the effectiveness of the AERAS approach, and of the training activities of the trainees, it is a integrated iterative process that involves several phases, starting from a pre-training preparation phase to the evaluation of results and adaptation of training activities and models.

Each task is supported by a specific AERAS tool or procedure, driving the trainers in the process. The schema in Figure 2, describing a checklist for the evaluation and adaptation techniques, can be considered strictly connected to WP3 “AERAS Models & Model-driven Cyber Range programmes creation” activities, since it considers the methodologies for the population of models.

The importance of the continuous monitoring and adaptation of training process to trainees results and performances has been explored in many seminal works [1] [2]. NIST, in the “Role-Based Model for Federal Information Technology/Cybersecurity Training” document [3], highlighted the importance of an evaluation process to develop information technology/cybersecurity role-based training. The primary focus of this process is to provide a comprehensive and flexible training methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities.

In the following, we are going to provide a short introduction of the five phases, that will be examined in the next sections, proposing for each task the specific AERAS tool or methodology of reference and the way the task will be tackled following our approach.

Figure 2: AERAS Evaluation and Adaptation Checklist.

***Phase 1: Pre-training***

The Pre-training phase will execute a first analysis of the security and risk profile of the pilot’s and an analysis of its specific training needs.

This phase is a pre-requisite for the definition of the training activities and the population of the CRSA models. In fact, an analysis of the vulnerabilities and risk detected in the Pilots will highlight on which aspects the training activities should be focused on.

The three task of the phase will provide inputs for the following phase. In particular, the open source vulnerability scanner OpenVAS[[2]](#footnote-3) will be exploited to define on which aspects the trainers have to focus during the definition of the training activities.

***Phase 2: Models Population***

The AERAS approach is based on the two foundation models: the **Cyber Range Security Assurance (CRSA)** models specifying potential cyber-attacks, the security mechanisms used against them, and the methods for assessing their effectiveness, and the **Cyber Range Simulation and Training (CRST) models**, describing the training activities composing the training programmes and whose definition is based on the CRSA data.

The structure of CRSA and CRST are subject of WP3 activities and will be described in D3.1 “CRSA Models and CRSA-driven Cyber Range programme specification language” and D3.2 “AERAS Models and CRSA-driven Cyber Range programme V1”.

The CRSA and CRST will be the base for the creation and execution of training activities. They will provide the goal and target of the specific training (CRSA) and the respective activities to be fulfilled (CRST).

***Phase 3: Training***

This phase will include the use of the platforms by the trainees that will complete all the activities that are assigned to them. The goals and contents of the training actions are described in the CRSA and CRST.

The results of the specific trainees are then collected and will be supplied as input for the following phase.

***Phase 4: Post-training***

In this phase two aspect are examined: the security and risk profile of the pilots after the training, and the aggregation of trainees results.

In particular, the change in the security profile can be an evidence of the effectiveness of the training activities, while a deeper analysis of students performances can determine the need of releasing alerts for the adaptation of the training activity.

***Phase 5: Evaluation & Adaptation***

The data collected in the previous phase are here analysed and analysed to actually evaluate the training activities and trigger adaption alerts.

At the end of a training campaign, the adaptation alerts received are used to improve the training activities raising, or lowering, the complexity of the exercise, or focus them on the aspects that the analysis of the security and risk profile still highlights as critical.

# Phase 1: Pre-Training Phase

As described in Section 2, this phase is dedicated on setting the stage for the foundation models of the AERAS framework. This phase is critical for the evaluation and adaptation process, but it is also of paramount importance for the definition of AERAS training activities.

The three tasks that compose the phase cooperate to collect all the data needed for the start-up of the framework and to semi-automatically identify the goals that the organization will best benefit form the training activities. The human support will be also critical in the definition of the specific training requirements and content.

In the following section, the discussion will focus on the specific tasks and the connection with the respective AERAS tool and methodologies.



## Task 1.1: Pre-training security and risk evaluation (tool)

This task is of paramount importance for setting the stage of AERAS training framework. In fact, the AERAS approach is founded on the concept that the effectiveness of the training actions can be evaluated basing on the improvement of the overall cybersecurity profile of the Organization. This approach has already proved as valid by the experimentation within the Horizon 202o project THREAT-ARREST and documented in its Deliverable 7.8 [4].

The task is implemented by the AERAS procedure “Cyber System Real Time Risk Evaluator” and in particular by the “Threat Assessor” (Figure 3). This procedure involves the use of the open source vulnerability scanner OpenVAS used to detect and report possible vulnerabilities and weak points in the organization’s system.



Figure 3: AERAS procedures implementing Task 1.1

The scan will produce a report containing a summary of the detected vulnerabilities, ordered by severity and based on the National Vulnerability Database[[3]](#footnote-4) (NVD) provided by the National Institute of Standards and Technology (NIST).

The set of discovered vulnerabilities, included in the OpenVAS report, as well as the information about the Common Vulnerability Scoring System (CVSS) rate and impact of these vulnerabilities, will be included in the instance of the CRSA model and used to shape and index the training activities. Details about the data to be collected and included in the instances of the CRSA models will be provided in D3.1 and D3.2.

In the context of the monitoring and adaption framework described in this deliverables, the analysis related to the cybersecurity posture of the organization are used to calculate the overall risk profile, whose trend during the training will be then used to evaluate the effectiveness of the actions.

In the “Cyber System Real Time Risk Evaluator” tool, in fact, taking in input the data provided by the OpenVAS report, an overall risk rate is calculated. In particular, the CVSS is used is reliable indicator of the cybersecurity risk rate of the pilot.

As described by Mell *et al.* in [5] , CVSS offers the following benefits:

* **Standardized vulnerability scores.** CVSS is application-neutral, enabling an organization to score all of its IT vulnerabilities using the same scoring framework.
* **Contextual scoring**. CVSS scores represent the actual risk a given vulnerability poses, helping them prioritizing remediation efforts.
* **Open framework**. CVSS provides full details regarding the parameters used to generate each score, helping to understand both the reasoning behind, and the differences among, vulnerabilities scores.

The goal is for CVSS to facilitate the generation of consistent scores that accurately represent the impact of vulnerabilities. The CVSS score is calculated composing different metrics that examine specific aspects of the vulnerabilities, such as impact, exploitability, damage potential (see Figure 4).

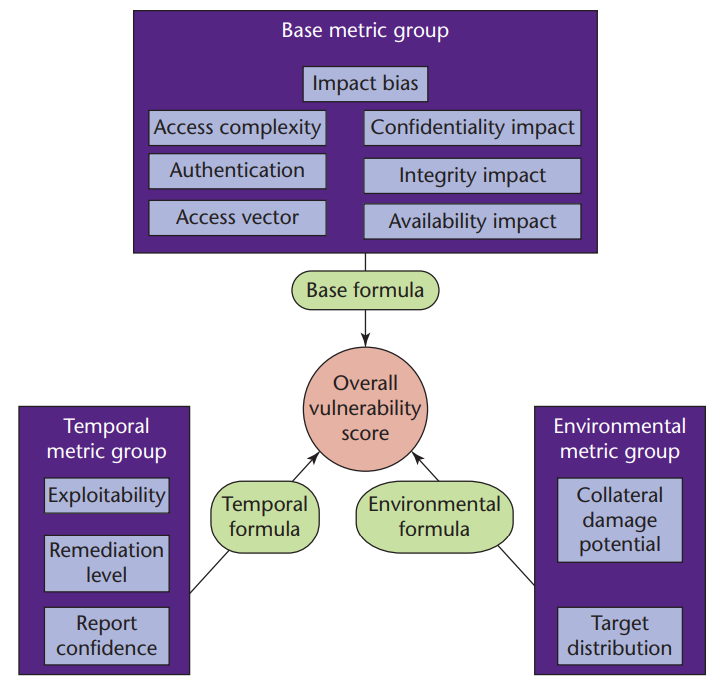


Figure 4: CVSS metrics composition [5].

One of the objectives of the AERAS project is to integrate in the proposed methodology, a mechanism for the continuous real-time monitoring of cyber-system and trainees[[4]](#footnote-5). The “Cyber System Real Time Risk Evaluator” tool will play the role of providing data about the actual state of the system. These data will be them proposed within the trainers interface in order to provide them the actual trend of the Organization’s security posture before, during, and after the training activities. Data shall be drilled up and down to visualize the aggregate rate, or the specific vulnerability CVSS value.

The tool will provide interface for launching the vulnerabilities analysis and aggregate the data, providing an unique indicator of the Organization’s risk rate calculate as:

Where *n* is the total number of detected vulnerabilities, *CVSS* is a function that identify and return the CVSS rate of the specific vulnerability *i* included in the OpenVas report, and *t* is the time when the rate has been calculated (*t=0* is the pre-training value). Furthermore, *severity* is a weight introduced to give more importance to vulnerabilities whose severity rate has been considered *High* (*severity=1*), other than *medium* (*severity=0.7*) or *low* (*severity=0.5*).

Data about risk level are then saved into a specific Risk Data database, that will be exploited also by Task 5.1 for post-training risk evaluation. The tool will also provide input to the Cyber System Multi-layer Monitor, that will use the provided data for CSLA continuous monitoring, and the data will be used in the population of the CRSA models. Figure 5 depicts the flow of data among the mentioned tools.

Cyber System Real Time Risk Evaluator

Cyber System Multi-layer Monitor

Visualization

CRSA models

*List of vulnerabilities with:  
- description  
- impact  
- solution*

*List of vulnerabilities  
RiskRate*

*List of vulnerabilities  
RiskRate*

Risk Data

Figure 5: Risk evaluation data flow.

## Task 1.2: Training needs analysis (procedure)

The *Training Needs Analysis* procedure is aimed at providing all the needed data used to complete the CRSA models and populate the CRST with the actual information about the training programmes. This work will be better detailed in WP3, but it is also important for the sake of the adaptation process since it will provide the baseline and the ground over which any adaptation actions will be based on.

In fact, the learning process can be seen as an iterative cycle where the trainers define the programs, apply them, collect feedback and then revise the programs with respect to trainees results and comments. More in details, the learning cycle can follow the so-called “Kolb’s Four Stage of Learning” [6]. Kolb proposed that a learner moves through a cycle of actions which leads to observations and reflections on the training activity. These reflections are then absorbed and linked with previous knowledge and translated into abstract concepts or theories, which result in new actions to adjust to the training programme that can be tested and explored. The author identifies the following four experiential learning stages:

1. Concrete Experience: This stage of the learning cycle emphasizes personal involvement with people in everyday situations. The trainees can be faced with real-world problems to test their reaction and develop their skills.
2. Reflective Observation: In this stage of the learning cycle, people understand ideas and situations from different points of view. The gained experiences are examined through different perspectives, the results are processed, their significance is understood, and conclusions are drawn.
3. Abstract Conceptualization: takes the reflective process a step further by focusing on channelling those observations into a set game plan or theoretical approach. The experiences gained in the previous stage are grouped, linked to scientific data and/or theoretic approaches, general principles are drawn, and action guidelines are formed.
4. Active Experimentation: this stage deals with the process of testing existing ideas by creating new experiences. For instance, in the abstract stage, a trainee might develop theories based off of observations learned in the reflective stage, and in the active stage, the leader takes the time to then test their theories.

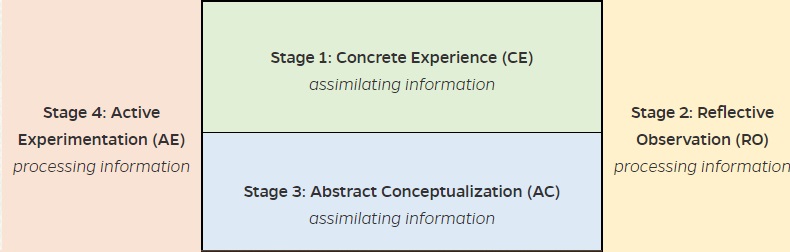


Figure 6: Kolb's cycle stages of learning.

In this iterative cycle (see Figure 6), the trainee’s evaluation has to be continuous, systematic, methodical, pedagogical, and multi-factor in terms of what has been taught, learned, and is capable of doing. Thus, an effective training procedure must be able to prepare a effective training programme that could foster the abstract conceptualization and experimentation of trainees. The programme should be also designed to adapt to each trainee’s capabilities and results, and continually contribute to their improvement.

The training needs of the Organization need to be evaluated, collected, examined and categorized in order to be included in CRST models and used as basis for the training programmes definition. Furthermore, the specific training activities identified in the analysis should be linked to the cybersecurity-specific concepts identified by the *Threat Assessor* procedure. This step will allow to link specific training activities to specific issues or weaknesses identified in the system, and will allow a monitoring of the system effectiveness based on the continuous assessment of the cybersecurity posture of the Organization.

# Phase 2: Models Population

The work in WP3 is focused on the definition of the structure of CRSA and CRST models, in turn defining the cybersecurity assets and concepts related to the organization, and describing the details of the proposed training programmes. A strict link between the two is expected, to index training activity to specific vulnerabilities (e.g., DDOS attack) or assets (e.g., firewall or email clients).

The preparatory work in Task 1.1 and Task 1.2 are intended to support the work in the following tasks, providing them with specific data about the pilot’s cybersecurity landscape and training requirements.



## Task 2.1: CRSA Models population (procedure)

This task is related to the population of CRSA models. In particular, CRSA models are organized in four submodels, each describing a particular aspect of the pilot’s cybersecurity landscape and better explained in WP3 deliverables. Namely, each submodel (depicted in Figure 7) it is of interest for the following aspects:

* **Cyber System Submodels**: include data relative to the assets of the Organizations interested at the cybersecurity level. These assets could be workstations, personal laptops, routers, servers, or specific software used by employees. The identification of such assets will be done exploiting information collected in Task 3.1, but also by specific interview and analysis on site.
* **Cybersecurity Assurance Submodel**: this submodel includes data related to the assurance level of the company, investigating aspect relatives to the certification and maintaining of a predefined cybersecurity Service Level Agreements, and indicating aspects to be monitored to preserve the requested security level.
* **Risk Assessment** **Submodel**: contains data related to the risks detected in Task 3.1 and their current value. This submodel is of paramount importance in the continuous monitoring of the overall risk level before, during, and after the training activities.
* Threats and Incidents Submodels: the submodels keeps track of specific cybersecurity threats, vulnerabilities and, if available, incidents. Threats and vulnerabilities can be referred in training activities definition in other to categorize them, while the incidents tracking can be of interest in providing hints on improving in the cybersecurity management reducing the number and severity of detected incidents.



Figure 7: CRSA Submodels.

At each iteration of the Evaluation and Adaptation checklist the value in the submodels can be updated with the new data coming from Task 3.1 and 3.2. The submodels themselves include a timestamping mechanism that allows trainers to follow and examine the trend in the cybersecurity landscape during the training activities.

## Task 2.2: CRST Models population (procedure)

The procedure described in Task 2.2 is the specular of Task 2.1 described above but related to the training activities specification and linked to the CRST Programme Generator module (Figure 8).



Figure 8: CRST Programme Generator module.

The definition of the training activities, and the consequent population of CRST models, is important and linked to the monitoring process since it categorizes the activities with respect to the cybersecurity aspects listed in the CRSA models.

In fact, the goals of training activities are mainly referred to the defence against specific threats that are described in the CRSA models. At the same time, the positive (resp. negative) modification in specific risk values can be related to the effectiveness (resp. ineffectivess) of the linked training activities.

The role of trainers in this phase is of paramount importance since they have to indicate which specific training activities the programme should include with respect to the cybersecurity landscape of the Organisation. In fact, trainers can supply a training programme that is strictly related to Organization’s needs, described in the analysis of Task 3.1 and interview with pilot’s cybersecurity managers, organized on concrete objectives (i.e. active threats or vulnerability), as well as on general cybersecurity concepts. Furthermore, the lay the basis of the monitoring and evaluation approach linking activities to the respective risk factors.

The procedure described in this task will be further explained in WP3 deliverables. It is important to note that the training activities can be performed exploiting asynchronous methodologies, such as administering to the trainees *ad-hoc* questionnaires, or exploiting the facilities provided by the internal AERAS cyber range. The two modalities, or a mix of the two, will be configured in the CRST and interpreted and enacted by the CRST programme Generator Module, part of the cyber range engine.

# Phase 3: Training

The training phase is composed by a single task (Real-time Assessment of Trainee performances) and is dedicated to the execution of the training activities and on the tracking of trainee results. This phase will rely on the facilities provided by the cyber range infrastructure, and on its ability to track the actions of students.



## Task 3.1: Real-time assessment of trainee performances (tool)

This task is mainly performed by the Performance Evaluator and Progression Engine tools of the AERAS stack (Figure 9).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Figure 9: Performance Evaluator and Progression Engine.

The Progression Engine, implemented following a Finite State Machine (FSM) architecture, is included in the Cyber range infrastructure and manage the administering of test and exercises during the execution of training activities. In fact, each programme, together with the support training material, are equipped with a set of activities (questionnaires and/or practical exercises on virtual environments) to be administered to the trainees. These activities are managed using an FSM approach by the Progression Engine.

The Progression Engine, during its execution, retrieve its inputs from the CRST Models and from the Cyber Range tools that manage the administering of the exercise to trainees. Then, the data are saved in a specific Training Results database to be accessed by the Performance Evaluator and all the tools that need to exploit trainees’ performance data (see Figure 10).

Performance Evaluator

CRST models

*Training Activity ID  
Training Programme ID  
Training-specific data*

Training Results DB

Progression Engine

Cyber Range Tools

Figure 10: Progression Engine expected communication flows.

# Phase 4: Post-Training

In this phase, the data collected during the execution of the training activities are aggregate and supplied to the other tools and procedures that need them to verify trainees progresses and evaluate possible adaptation alert on training programmes.

The phase id compose of two task, dedicated to the re-evaluation of the security landscape after the execution of the training, and the production of aggregate statistics about the trainees.



## Task 4.1: Post-training security and risk evaluation (tool)

Task 4.1 replicates the procedure describes in Task 1.1, where the cybersecurity landscape of the Organization administering the training programme is examined. The goal of the step is to understand if and in which measure the training activities helped in reducing the calculated risk level of the Organization.

The flow proposed in Figure 5 is still used, with the difference that there is a comparison between the data related to the pre-training phase, and the current data calculate in post-training. Figure 11 depicts the new scenario.

In this task, only the vulnerabilities and risk detected in Task 1.1 are taken into consideration, and the interaction with CRSA models is related to the retrieving of input data only. Moreover. The status of the improvement (resp. deterioration) of the cybersecurity landscape of the Organization will be proposed by the Visualization in specific panels.

Cyber System Real Time Risk Evaluator

Visualization

CRSA models

*List of vulnerabilities with:  
- description  
- impact  
- solution*

*Updates on RiskRate*

Risk Data DB

Figure 11: Post-training risk evaluation flow.

Since the checklist proposed in this deliverable is designed to be iterative, during each round the new risk data calculated in each iteration are saved in the Risk Data database to have the actual trend of the cybersecurity landscape. For this reason the interaction between the Cyber System Real Time Risk Evaluator and the Risk Data database are both in input and output.

The risk data will be proposed together with the data related to the trainees training activities, in order to provide the trainers with an effective tool to find and examine possible correlation among training activities and solved (resp. still active) vulnerabilities.

## Task 4.2: Production of aggregate data on trainees' activities

The Performance Evaluator tool, in cooperation with the Progression Engine, evaluates and aggregates the data saved in the Training Results Database. These data, in explicit or aggregate form, are sent to the Visualization tool for providing specific information about the performance of the trainees, or general aggregated data about the training programme (*no. executed training activities, no. active trainees, mean-min-max test results, …*).

Furthermore, data about performance are also of importance for the Programme Adaptor tool that will exploit the usage data and test results to raise alerts about the need of adaptation of training programmes. Further information about the Programme Adaptor will be provided in Section 7.

Performance Evaluator

Programme Adaptor

Visualization

CRST models

*Training Activity ID  
Training Programme ID*

*Trainee ID  
test results  
Execution time  
Training ID  
TrainingProgramme ID  
aggregatedTestResults (trainingID)  
aggregatedExecTimes(trainingID)*

*Training ID  
TrainingProgramme ID  
aggregatedTestResults (trainingID)  
aggregatedExecTimes(trainingID)*

Training Results DB

Progression Engine

Cyber Range Tools

Figure 12: Performance Evaluator tool data flow.

Figure 12 depicts at high level the communication flow cantered on the Performance Evaluator tool. In particular, the tool will exploit data saved in the Training Results database in order to produce an aggregation of data related to the execution of training activities.

On one side, the visualization tool should be able to display data in both aggregated and punctual forms. The trainer should be able to see the progress in term of *trainee* (punctual) and in term of *training programme* as a whole (aggregated).

On the other side, the Performance Evaluator will share aggregated data with the Programme Adaptor tool, that in turn will use the data to evaluate the level of accomplishment of the training programme, indicating the need (or not) to send alerts with respect to required modifications and amendments to specific training activities.

It is important to note how the use of aggregated data in the adaptation phase will preserve the privacy of the specific trainees’ training data.

# Phase 5: Evaluation & Adaptation

This phase deals with the evaluation of the data coming from the previous phase, in order to assess possible change in the construction of the training programme and the effectiveness of the programme itself.

One of the key point of the AERAS framework is its intrinsic ability of providing an assessment *on-the-field* of the effectiveness of the training programmes. This is implemented thanks to the continuous assessment of organization’s security landscape and risk levels, and the link between training activities and detected vulnerabilities, through the CRSA models.

The following tasks describe how the comparison is made and the mechanism that will send alerts on training activities that need to be adapted.



## Task 5.1: Pre- and Post-training security and risk comparison (tool)

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamenteTask 5.1 is related to the comparison of risk data collected before in Phase 1, and the risk data as output of the Phase 4. The task goals are enacted by the Training Performance Monitor tool (Figure 13).

Figure 13: Training Performance Monitor tool.

During Phase 1 and 4, data about risk evaluation are saved into the Risk Data DB. The tool will make a comparison about the data at different time slice, highlighting the improvement (resp. deterioration) of the security landscape. Risk data are connected to the respective vulnerabilities and, thanks to CRSA models, to the assigned training activities.

Comparison data are then saved in specific monitoring tables and/or views to allow a quick visualization of data, giving the possibility to drill up and down with respect to specific training activities.

The following Figure 14 provides an overview of the expected communication flow of the tool. The data related to the comparison will be mainly exploited by the visualization interface, in particular in for the trainers view, and by the Programme Adaptor module for the issuing of specific adaptation alerts.



Figure 14: : Training Performance Monitor expected communication flow.

Training Performance Monitor

Visualization

CRSA models

*List of vulnerabilities with:  
- description  
- impact  
- solution*

*riskRate(timePeriod)*

Risk Data DB

Programme Adaptor

*riskRate(timePeriod)*

CRSA models

*Training Activity ID  
Training Programme ID*

## Task 5.2: Adaptation Analysis of training activities (tool)

Immagine che contiene testo, Carattere, simbolo, segnaletica

Descrizione generata automaticamenteDuring Task 4.2, aggregate data about trainees results and usage, with respect to specific training activities, has been already made available to the Programme Adaptor tool. In this task, we describe at high level how the programme adaptor is going to evaluate these data in order to identify training programs or training activities that need to be adapted.

Figure 15: Programme Adaptor tool.

The Programme Adaptor can detect needs of adaptation in case one or more of the following conditions are detected:

* **Change in Company assets**: during Task 2.1, CRSA model are populated with the list of detected vulnerability and the assets of the Organization that are subject of cybersecurity controls (e.i., firewalls, routers, critical workstations). Any time there is a change in the topology and a new asset is detected, the condition is met and the Programme Adaptor will trigger an *AssetChanged* alert. This condition is required since new assets present in the Organization topology could requires new skills and training to manage them.
* **New vulnerability found**: if in a iteration of the Task 1.1 a new vulnerability is found that it was not part of the original sets, the *NewVulnerability* alert is triggered in the Programme Adaptor. The alaert is an important notification, since the new detected vulnerability could raise the Company risk factor and change the overall cybersecurity landscape. New training activity should be added to the programme in order to deal with the new threat.
* **Low trainee performances**: if the Programme Adaptor detect a level in trainee performance lower than a specified threshold, the *LowPerfomance* alert will be triggered to notify trainers of that situation. Trainer then can analysis usage trainees data in order to identify if the low perfamcne is due to a low commitment of trainees in executing training activities, or of a too-high complexity of the exercises that should be adapted.
* **High trainees scores**: if the Programme Adaptor detects that the trainees results is on average over a predefined threshold (i.e., 90% of the maximum grade), the *HighScore* alert is triggered. This alert can notify to the trainers that the overall training programme is too simple for the average level of trainee and, to optimize training outcome, the activities should be adapted to cover an highest level of complexity.
* **High (resp. Low) completion times:** this condition is met when the average time needed to complete the training activities are above (resp. below) a predefined percentage threshold of the maximum time expected to complete the training. If the condition is met, the *HighCompletionTime* (resp. *LowCompletionTime*) alert is triggered suggesting adaption to the specific training activity.

Task 5.3 deals with the actual sending of the alerts that have been triggered during this task analysis. The communication flows in Figure 12 and Figure 14 already depict the input flows used to feed the Programme Adaptor tool.

## Task 5.3: Alerts on training adaptation needs

In this task the Programme Adaptor collects all the alert messages that the tools in Task 5.1 and 5.2 has sent, providing them to the visualization in order to be notified to the trainers.

The diagram in Figure 16 depicts the communication flow between the Programme Adaptor and the Visualization. In particular, the Programme Adaptor will send the collected alerts with the specification of the alert category, specific training activity involved or new vulnerability/assets (objects) detected, and the sending timestamp. For each kind of alert, a template of alert message will be included in order to provide more information to the trainee.

It is important to note that the role of the Program Adaptor will end with the sending of the alerts. The actual implementation of the adaptation action will be on the responsibilities of the trainers and managers. In the next iteration of the checklist, the tool will provide alerts only on newly detected adaptation actions, without repeating the same notification twice.

Figure 16: Programme Adaptor expected communication flow.

Visualization

*List of alerts with:  
- type of alert  
- object involved  
- template message  
- timestamp*

Programme Adaptor

The Programme Adaptor close the cycle of the Evaluation and Adaptation checklist, that can be iterated by the organization when the course is updated or after the termination of the training programme. Trainers and managers can decide to iterate the checklist also in case of the evidence of new threat or vulnerabilities that can involve the organization. The new iteration will update the current CRSA models and, if the training programme needs changes, the current CRST models.

# Conclusions

This deliverable presented the Evaluation and Adaption checklist that describe and implement the AERAS methodology that provide the mechanism for the continuous evaluation and adaption of the training programmes.

The iterative methodology involves most of the tools and procedures of the AERAS frameworks, and details the relation and the communication flows among the tools.

This deliverable constitutes a preparatory work to lay the basis also to the overall AERAS infrastructure, that take as its strong point the correlation between the improvement of the cybersecurity landscape of the adopting organizations, and the effectiveness of the administered training programmes.

# References

|  |  |
| --- | --- |
| [1] | G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis and H. Koshutanski, “Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees,” *Applied Sciences,* vol. 10, no. 16, 2020. |
| [2] | D. Kirkpatrick and J. Kirkpatrick, Evaluating Training Programs: The Four Levels, Berrett-Koehler Publishers, 2006. |
| [3] | P. Toth and P. Klein, “A Role-Based Model for Federal Information Technology/ Cybersecurity Training,” National Institute of Standards and Technology (NIST), 2014. |
| [4] | THREAT-ARREST Project, “D7.8: Final THREAT-ARREST evaluation report,” 2021. |
| [5] | P. Mell, K. Scarfone and S. Romanosky, “Common Vulnerability Scoring System,” *IEEE Security & Privacy,* vol. 4, no. 6, pp. 85-89, 2006. |
| [6] | D. A. Kolb, Experiential Learning: Experience as the Source of Learning and Development, Pearson FT Press, 2014. |

1. † *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.* [↑](#footnote-ref-2)
2. <https://www.openvas.org/> [↑](#footnote-ref-3)
3. <https://nvd.nist.gov/> [↑](#footnote-ref-4)
4. **Objective 2:** Develop **novel hybrid cyber security risk analysis models**, which **combine** traditional **static cyber security risk analysis** principles and standards with **continuous risk estimates**. These estimates are informed from **simulation** and the continuous **real-time multi-layer monitoring** of cyber-systems and trainees. [↑](#footnote-ref-5)