Ref. Ares(2019)7074440 - 15/11/2019


**Marie Skłodowska-Curie Actions (MSCA)**
**Research and Innovation Staff Exchange (RISE) H2020-MSCA-RISE-2019**

**Project Acronym: AERAS – Project Number: 872735 Annex 1 to the Grant Agreement**
**(Description of the Action) Part B**

# 1. Table of Contents

# 2. Excellence

## 2.1 Quality and credibility of the research/innovation project; level of novelty and appropriate consideration of inter/multidisciplinary, intersectoral and gender aspects

### 2.1.1 Background and Motivation

Healthcare is one of the critical sectors in the Directive on Security of Network and Information Systems (NIS Directive), the first EU-wide legislation on cybersecurity [1]. In 2016, government **expenditure on health** in EU-28 reached **7.1% of EU GDP**, exceeding other critical sectors in the NIS Directive, namely transport 1.9%, fuel and energy 0.3%, communication 0.05%, economic affairs 0.9% [2], but also expenditure in defence and education combined (1.3% and 4.7%, resp.) [3]. Healthcare has undergone dramatic changes in the past years as it capitalizes on digital advancements to improve overall patient experience and outcomes: adoption of e-health records (EHRs), increased use of medical applications, online patient portals, connected devices, and wearables.

As technology use in healthcare grows, so do cyber-attacks. Personal health information (PHI) and EHRs stored in healthcare organisations are of incredible value to cybercriminals, as they contain personal information (e.g. social security numbers and insurance information) that can be easily used for fraudulent purposes or sold for profit. Also, risks are too high with medical devices, especially smart wearable devices and implants (e.g., drug infusion pumps, defibrillators), which interact with the physical world and affect patient health directly. **Healthcare industry** was ranked in the lowest industry performers group (**6th lowest**) in terms of **"security performance"** by the U.S. State and Federal Government in 2017 [4], and was a the **most targeted by ransomware** (accounting for 88% of ransomware detections) as found by the Solutionary Security Engineering Research Team (SERT) [5]. Also, the HIPAA journal [6] reported **yearly increases in healthcare data breaches**, while security researchers have successfully hijacked tele-operated surgical robots [7], tampered with drug infusion pumps [8], and have identified tens of thousands of vulnerable online medical systems [9][10].

Nevertheless, addressing these security challenges is not a trivial task. There are numerous and complex **security vulnerabilities** not only due to a **lack of** systematic application of a **common security policy**, but also from failure to understand the **complex interactions** between patients, clinicians and healthcare professionals, careers, administrators, software and medical systems, services, and devices, and their **security implications**. **Security gaps** are further **exacerbated** by the continually **evolving nature** of **medical systems technologies**. The lack of cyber resilience in the healthcare sector is also affected by the **lack of** appropriate **training** for developing and sustaining the expertise in preventing and recovering from increasingly sophisticated cyber-attacks for different personnel and stakeholder types within healthcare organisations [11][12]. This is a **severe gap** given that healthcare organisations are increasing a target of cyber attackers [13].

However, although the need for **cyber security training** is **essential**, the **effectiveness** of **existing security training** schemes is **questionable**. More specifically, as indicated by surveys, many healthcare organisations do not offer security awareness training to their personnel at all and consistently consider the investments made in such training as inadequate [14]. This is particularly surprising, since security awareness measures are subjectively evaluated as the most effective by organisations [15]. Furthermore, security awareness and training programs should be tailored to an organisation's specific and ever-changing needs and environment, based on a needs-assessment conducted for this purpose [16].

In addition to the above, healthcare organisations, like in other sectors, find it particularly challenging to **estimate the likelihood** and *impact of cyber risks* and **assess the cost and benefits of** alternative **security mechanisms** for mitigating such risks. Most of the risk assessment methods rely on estimates that do not use real data from the continuous monitoring of systems. It is widely recognised, though not enforced by current standards and regulations, that security assurance programme must rely on the **continuous** and **automated monitoring** of systems and processes [17], so as to inform the cyber security training. Also, organisations should take advantage of complementary security mechanisms, like **cyber security-focused service level agreements** (CSLAs) CSLAs are particularly important to **commit providers** of external components, devices, and services to **guarantees about** the **security** resilience of their offerings and specific **penalties** if these guarantees are violated [18][20].

Thus, the orchestrated use of all the available cyber security risk exposure mitigation mechanisms (hereafter referred to as "security controls" for the sake of brevity), including CSLAs, typical cyber security mechanisms and controls (CSCs) and cyber security training, can provide far more effective coverage of organisations against cyber risks.

### 2.1.2 Aim and specific objectives

Motivated by the above, AERAS aims to:

Develop a realistic and **rapidly adjustable cyber range platform** for systems and organisations in the **critical healthcare sector**, to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical cyber-systems and organizations against advanced, known and new cyber-attacks, and reduce their security risks. The platform will be a virtual cyberwarfare solution enabling the simulation of the operation and effects of security controls and offering **hands-on training** on their **development**, **assessment**, **use** and **management**.

The platform will be based on an evidence-based approach where virtual cyberwarfare and simulations are configured according to evidence regarding: (i) the occurrence of cyber threats, and (ii) the effectiveness of the operation of the internal and external system defence mechanisms. Evidence will be collected by multi- faceted real- time monitoring and assessed according to Cyber Range Security Assurance (CRSA) models specifying potential cyber-attacks, the security mechanisms used against them, and the methods for assessing their effectiveness. The AERAS solution will be delivered at TRL-7 and validated through two different pilots in the healthcare sector: (i) a hospital medical systems pilot; and (ii) a public health systems pilot.

To achieve its overall aim, AERAS will pursue the following objectives:

***Objective 1**: Develop **Cyber Range Security Assurance models (CRSA models)** to drive the generation of **Cyber Range Simulation and Training (CRST) programmes**.*

**Description**: The delivery of cyber range training in AERAS will be based on CRSA models (defined & developed in T3.1 & T3.2). These models will define: (1) the cyber-system, (2) the threats for this system and the security mechanisms mitigating risks arising from the threats (i.e., cyber security controls, cyber security SLAs, and cyber security training); (3) the ways to assess the risks of this system; and (4) the ways to measure the impact and cost of threats and the cost of the security mechanisms used against them. Hence, CRSA models will be the backbone in generating cyber range simulation and training programmes.

**KPIs**: **KPI-1**: Deliver a language and an editor enabling the specification of CRSA models; **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); **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; **KPI-4**: Deliver at least 4 CRST programmes to cover the two pilots and two different user types for each of those.

***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.*

**Description**: The AERAS hybrid cyber risk analysis models (T3.4) will combine traditional security risk analysis (based on static security risk analysis and subjective probabilities of security threats occurrence and successful defences of security mechanisms) with evidence and simulation-based risk models. Evidence-based risk models will produce risk estimates from real evidence obtained through the continuous monitoring of attacks that are launched upon cyber-systems, and the effectiveness of the mitigation mechanisms used against them. Simulation- based models will be used to analyse risks by simulating cyber-attacks, the behaviour of the security mechanisms defending them, and the routes through which an attack may propagate within a cyber-system affecting its assets. Hybrid risk analysis will be defined as part of CRSA models, using the language developed in Objective 1.

**KPIs**: **KPI-5**: Delivery of at least 5 hybrid cyber-security risk analysis models, covering testing, static analysis, inspection, monitoring, and simulation based analysis, and capable of providing real-time risk estimates for all types of risks and security mechanisms identified in the pilots; **KPI-6**: Evaluate the effect of the use of hybrid cyber-security risk analysis models for the timely adaptation of risk analysis, with new outputs for new required controls produced within minutes of new information becoming available.

***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.*

AERAS will support the **adaptation of** cyber range simulation and training (CRST) **programmes** (T4.6) and the

**CRSA models** used for their generation (T3.3). These adaptations will typically include changes to configuration parameters of a programme to make it more or less challenging (e.g., increasing simultaneous attacks, eliminating certain security mechanisms or adding more) or to values of the models underlying the generation of CRST programmes (e.g., changing the default rate of threat occurrence or the probability of a cyber-insurer rejecting a claim related to a particular security incident). Such **adaptations** may be applied **at** the **individual trainee level** (CRST programme personalisation) or at **CRST programme level**. To support adaptations, AERAS will rely on the **integration of multi-layer monitoring mechanisms** (T4.5) capturing and analysing events from all layers of the organisation, such as cyber-system end-points, network (e.g., through intrusion detection) and applications (e.g., application availability). Moreover, once instantiated, CSLAs will be monitored by AERAS for compliance and coverage, and trigger adaptations when necessary. In addition, mechanisms will be developed to **capture and analyse the performance of trainees who undertake CRST programmes** (T4.3); e.g., time spent on exercises, ratio of successfully completed exercises, ability to reach some level of difficulty, progress of performance over time.

**KPIs: KPI-7:** Delivery of the monitoring and adaptation mechanisms of CRSA models and associated Cyber Range programmes; **KPI-8:** Delivery of real-time monitoring mechanisms to support the pilots. The mechanisms should cover all monitorable security mechanisms, security risks and trainee actions defined in the CRSA and models and CRST programmes developed for the pilots; **KPI-9:** Demonstrate at least 6 sets of adaptations, covering all feedback loops from CRST programme performance, CSLA and Cyber-System monitors (one for each of the monitored layer).

***Objective 4:*** *Develop capabilities required for the delivery of effective* ***cyber training****, namely* ***emulation****,* ***simulation****,* ***security assurance assessment****, and* ***visualisation*** *capabilities.*

**Description: Emulation and simulation** capabilities (T4.1) will enable the AERAS platform to mirror instances of the actual physical/software components of a cyber-system (e.g., networks and data servers) and allow trainees to interact with the emulated components (e.g., log in a virtual machine) and perform certain operations (e.g. divert traffic flow) to react to attacks. The components of a cyber-system that can be simulated or emulated and their configuration, as well as the effects of the operation and of user actions upon these systems and components, and the launch of security attacks against them, will be defined via CRSA models. Moreover, **Security assurance** (T4.4) capabilities will be used in AERAS to provide a continuous real time analysis of the security status of the cyber-system and the organisation that the training targets. Moreover, **Visualisation** (T4.2) capabilities will be developed for AERAS users to interact effectively with cyber training, using appropriate visualisation metaphors for different types of attacks and system components, enabling zoom-in and out views of the system, and be interactively and intuitively controlled by trainees.

**KPIs: KPI-10:** Delivery of mechanisms enabling the emulation and simulation of all key types of cyber system components, including external devices, web servers, data base servers, security servers, event busses, operating systems, trusted platform modules, and network components; **KPI-11:** Delivery of mechanisms enabling the assessment of the emulated and simulated component's security assurance status and the actions performed on them by the trainees; **KPI-12:** Delivery of visualisation tools covering the state of the simulated/emulated cyber systems; the attacks upon them; the effects of user actions; comparative performance measures (e.g., individual trainee performance vs group performance, performance over different time periods, performance for different threats/attacks) and the capability to zoom in and out on parts of the system and the events related to them.

***Objective 5:*** *To* ***integrate*** *capabilities developed under Objectives 1-4 into a common platform that delivers* ***realistic*** *and* ***highly adjustable cyber training****, offering* ***hands-on experience*** *against cyber-attacks, and supporting* ***decision making*** *in* ***employing different*** *mixtures of* ***security mechanisms*** *to combat* ***risks*** *and to* ***demonstrate and validate*** *the use of the AERAS platform for realistic and highly adjustable cyber training in the critical healthcare sector using two separate pilots based on real systems at TRL 7.*

**Description:** The individual *AERAS* capabilities that will be developed under *Objectives 1-4* will be integrated to construct a fully functional and usable Cyber Range platform (T5.1). The functionalities of the *AERAS* platform will be offered through open APIs. The final platform will be delivered at **Technology Readiness Level (TRL) 7**, and validated through its two pilots. of AERAS. More specifically, the AERAS pilots will include: (1) a **hospital system** involving interactions with **patients** and **medical devices** (**Pilot 1**, T5.3), and (2) a **healthcare authority platform**, interconnected with hospitals and healthcare professionals spanning a large geographical area (**Pilot 2**, T5.4). The selected pilots use different cyber-system platforms, types of smart objects, devices and types of networks (including intra- and inter- domain communications). They also involve end users both of public and private organizations, and cover a significant spectrum of different (in terms of type, significance, and expected level of enforcement) security requirements, thus enabling a comprehensive evaluation of AERAS platform. The overarching target of validation will be to assess the platform's ability to increase stakeholder effectiveness against cyber-attacks in the healthcare

and other critical domains. This will cover all different types of responses: preparedness, incident detection and analysis, real time incident response, and post incident response.

**KPIs: KPI-13:** Delivery of an integrated cyber range training platform, with capabilities described in Objectives 1-4, at TRL7; **KPI-14:** Delivery, demonstration and evaluation of the integrated solution to each of the two pilot environments. **KPI-15:** Validation across 2 pilots, involving a total of 640 hours of training (20 participants x 16 hours x 2 pilots).

***Objective 6:*** *To ensure the* ***dissemination and communication*** *of the project's results and the* ***uptake*** *of the AERAS innovation to organisations in critical domains, and cyber security stakeholders.*

**Description:** This objective is to effectively disseminate and communicate (T6.1) the project outcomes in scientific conferences, industrial exhibitions and other related fora, and the general public. Moreover, it focuses on fostering a community of cyber-systems security and security solutions stakeholders (T6.2), critical cyber infrastructure owners and security auditors who will work on providing CRSA models for the delivery of effective Cyber Range training beyond the scope covered and training offered in the context of the *AERAS* pilots.

**KPIs: KPI-16**: Achieve the project's dissemination targets, as defined in Sect. 3.3.3; **KPI-17**: Achieve the project's communication targets, as defined in Sect. 3.4.

### 2.1.3 Novelty, level of ambition and foundational character

The current state of the art and practice in the areas targeted by AERAS is the following.

**Security Assurance Models:** Security assurance acquires evidence that infrastructure demonstrates some security properties despite failures and attacks [21], using (i) self-assessments by the infrastructure provider, or (ii) third party auditing. Khan et al. [22] present a continuous monitoring certification approach, while Bolgert et al. [23] a hybrid model, combining monitoring and testing. Anisetti at al. [24][25] evaluates testing-based evidence with a template-based approach. In certain cases, attack models must be evaluated or simulated, complicating things due to the fundamental differences between threat and attack models: the former explore the possibility of an attack, while the latter describe how vulnerabilities are exploited by malicious parties. Many focus on modelling threats such as OWASP (owasp.org), ENISA Threat Taxonomy [26] and IETF's RFC 2828 [27] but attack behaviour and actions need to be captured, analysed, and classified for a security assurance evaluation. In Anisetti at al.'s [28] test-based assurance approach for web services, attackers are modelled using five attacker capabilities [29] and finite state machine automata. Zulkernine et al. [30] use a model-based approach for automatically testing attack scenarios. Finally, Jurjens' [31] UMLsec-based systematic testing of security-critical systems generates tests to identify security weaknesses. *In AERAS, security assurance models will be extended by including coverage of CSLAs and novel risk models. Also, the modelling of system components will include parameters necessary for simulation along with explicit risk assessment models. AERAS aims to articulate CRSA-driven training programmes on security assurance models and use information acquired from continuous assurance evaluation so as to develop realistic simulations for Cyber Range training programmes. Also, its vision is to use continuous monitoring of assurance schemes to measure the trainees' performance.*

**Cyber Range Training:** High-quality cyber ranges recreate the experience of responding to a simulated cyber-attack by replicating the Security Operations Centre (SOC) environment, the organizational network, and the deployed attack [32]. Recent works [33][34] focus on developing an efficient cyber range platform and Damodaran et al. describe how cyber modelling and simulation is utilized in cyber-range events. The Cyberbit Cyber Range (cyberbit.com/solutions/cyber-range) is a training/simulation platform for the instantiation and management of hyper-realistic training centres, while AIT Cyber Range (ait.ac.at/en/research-fields/cyber-security/cyber-range) offers a virtual environment of flexible simulation of critical IT systems. The Virginia Cyber Range (virginiacyberrange.org/) is a cloud-hosted virtual environment for training students in handling cybersecurity events. The Michigan Cyber Range (merit.edu/cyberrange) focuses on strengthening Michigan's cyber defences and is one of the largest unclassified, network accessible cybersecurity training platforms, while the National Cyber Range (NCR) provides the ability to conduct realistic cybersecurity testing, evaluation (T&E) and training (acq.osd.mil/dte-trmc/ncr.html). *AERAS will develop and offer a novel approach to Cyber Range training, enhanced by its evidence-based CRSA models-driven approach. The cyber range training will not only encompass the realism provided by modern simulation, emulation and visualisation capabilities, for immersive virtualisation of cyber infrastructures and the associated cyber exercises (e.g. CTF), but will also adapt based on the continuous cyber system and threat landscape monitoring, the associated security mechanisms' cost/benefit assessment, and the programme and trainee evaluations. Thus, AERAS will offer a more effective training environment, tailored to the organisation and its more urgent cyber threats, and also provide an evidence-based, quantitative assessment of the effectiveness of the training programme, allowing its accurate cost/benefit analysis and optimization as a security risk mitigation mechanism.*

**Cyber Security risk estimation:** Guidelines for the risk management process are widely available and pay particular attention to organisational questions, such as the description of the parties involved, definitions of the main terms, the supporting documents, and high-level descriptions of the phases. Some guidelines are generic, not delving into the risk assessment and risk treatment phases [35], whereas others suggest possible techniques [36] and provide tools for risk assessment [37]. Guidelines also include other activities, such as implementation of treatments, communication of results, monitoring and assessment, maintenance and improvement. In this respect the overall cyber risk management process is an application of the widely known Plan-Do-Check-Act (PDCA) cycle. The ISO/IEC 27001:2013 can also be seen as a risk management guideline, as it covers most of the typical steps in risk management, including risk assessment and risk treatment. A number of approaches [38][39][40][41] define and support the implementation of the risk assessment and treatment phases in risk management, with an apparent consensus on the overall risk assessment and treatment process, despite some differences in the level of detail used to define the risk assessment steps or their names. *AERAS will integrate SLA and monitoring to continuously assess cyber-risk. AERAS models will map observable factors to incidents' impact and likelihood based on current evidence rather than on past history alone. This approach will exploit the observables made available by the monitoring capability of the project together with the current business value of information assets. AERAS innovation with respect to the state of the art is twofold: (i) enable continuous value-based assessment of assets, considering their evolution value, tailoring AERAS impact estimates to specific situations; (ii) use aggregation of individual assessments to reduce uncertainty in incident impact and likelihood.*

**Real-time Security Monitoring, Assessment and Event sharing mechanisms:** *AERAS* focuses on continuous evidence-based security assurance, through continuous monitoring and/or testing approaches. Test-based evidence is important for software assurance [42] and recently applied to assurance scenarios on services [43][44] and distributed systems [45]. Monitoring can be easily applied on the real operational system as it uses passive inspection. Automated assurance, continuous monitoring, smart evidence aggregation and evaluation have recently been hot topics for both industry and academia. Koschorreck [46] focused on automated audit and security controls with particular attention to models and standard protocols to represent and exchange audit results and operations. Startups, such as Moon-Cloud.eu link security assurance monitoring and testing through a distributed ecosystem of probes to implement security controls [47]. Moon Cloud also targets IoT environments [48], as do others [49][50]. An important aspect of monitoring is the sharing of the logged information regarding security incidents and threats. However, this practice can reveal vulnerable components of the Cyber-Infrastructure to adversaries. In the literature, there are sharing systems preserving specific characteristics [51][52]. Bodies like CERTs (Computer Emergency Response Teams) and CSIRTs, a reliable and trusted single point of contact for reporting computer security incidents and response worldwide, provide information on emerging threats and security incidents to any user. Other repositories share information about vulnerabilities and exploits and mitigation patches like CVEs. NIST NVD, adopts taxonomies and metrics to classify vulnerabilities in terms of Weaknesses (CWE) and in terms of severity (CVSS). *The AERAS's platform will deploy a novel three-layered monitoring system to assess the security of an organisation infrastructure in real-time. This will include end-points (e.g. devices monitored for misconfigurations) and the network infrastructure (e.g. monitored for intrusions). It will also monitor applications (e.g. through runtime monitoring tools) and also inspect the compliance of the end-user behaviour to specific organisational processes and their requirements (e.g., regulatory requirements). The above inputs will be aggregated to help update the pertinent sub- models and adapt the AERAS platform accordingly.*

**Cyber Security Service Level Agreements:** SLAs help govern service provider/consumer interactions and are strongly connected to Risk Assessment, as thresholds and alarms should be defined through declared/agreed SLAs [53]. Indeed, risk assessment and SLA fulfilment has been extensively studied [56], with complex services analysed by aggregating risk values of sub-services [54][55]. In information security and privacy [57] risk can be seen as a basis for proactive/reactive service management, as risk can be defined and linked to existing ways of expressing security policies [58]. Thus, one can associate policy events with proactive/reactive actions to reduce a risk [59]. *AERAS will use CSLAs as an integral part of the risk mitigation arsenal available to the organisation, assisting in the generation and deployment of the required CSLAs. After instantiation, the respective monitoring module, will acquire additional real-time information on the security of the healthcare organization by monitoring the specified CSLAs terms. The tools will also include provisions for dynamically allocating monitors to CSLA parts, based upon matching the exact agreement/policy terms, respectively, that need to be monitored and the monitoring capabilities available for different target systems and services. The output of the tools will be modelled to include each element in the Service Level Agreement, along with its specifications (scope, positive/negative results), the events that require monitoring, whether a suitable configuration is produced, and whether any violation or service request and response events are successfully captured. In addition to helping organisations more efficiently cover their cyber security risk exposure, this evidence-based strategy in the CSLA definition and compliance monitoring will help organisations demonstrate due diligence to relevant stakeholders (3rd parties, regulators etc.).*

Moreover, beyond the advancements to the state of the art in individual technology and scientific areas above, the overarching ground-breaking objective of *AERAS* is to deliver a platform that prepares stakeholders in defending high-risk, critical healthcare cyber-systems and organisations from advanced known and new cyber threats, while allowing them to effectively and efficiently manage the associated risks. This is achieved through the three novel key *AERAS* pillars, namely: (i) the provision of insights on the complementary exploitation of CSCs, CRST programmes, and CSLAs as risk mitigation measures against cyber security risks; (ii) the systematic assessment of security requirements and cyber security risk exposure estimation, towards the identification of the correct mixture of the above controls; and (iii) the *AERAS* cyber range training and simulation programme, which enhances security awareness and preparedness with a hands-on approach and with evidence to support the results of said training.

### 2.1.4 Methodology

**Basic Characteristics and Process of Generating CRST programmes**

*AERAS's* cyber range simulation and training (CRST) programmes will have two key characteristics:

***(1):*** *Be aligned with the overall security assurance programme that is (or should be) in place within an organisation*

A **security assurance programme** comprises risk assessment processes for detecting threats and evaluating the effectiveness of security controls of the cyber-systems and the overall security status of an organisation. As CRST programmes must **cover all** the known **security risks** of an organisation and be **adapted** based on **evidence** from the continuous assessment of the security status of the organisation's systems and processes, it is important to be aligned with its security assurance programme. To ensure this, AERAS CRST programmes will be generated from the specification of the organisation's systems and assets, the known threats and risks, and the security mechanisms established to protect it against the risks, as specified in cyber range security assurance (CRSA) models.

***(2):*** *Cover all the distinct security mechanisms that are available to organisations, and train stakeholders not only to use them correctly but also to combine them in the most cost effective way to cover against security risks*

Security protection could be seen a **decision-making problem** in which **cyber security risks** are allocated **onto** one or more of the **security mechanisms** (i.e., CSCs, CSLAs, and security training) that can handle them. Making such decisions requires stakeholders to develop a systematic understanding of the security requirements and other constraints (e.g., supplier dependencies, applicable regulatory frameworks) that may dictate or preclude the use of different security mechanisms. Hence, CRST programmes should train stakeholders with appropriate responsibility in organisations to **understand** and **assess** the **effectiveness** of **different security mechanisms**, and the **dependencies** and **complementarities** between them.

Figure 1 shows the overall *AERAS* process for generating and delivering cyber range training and simulation programmes. This process has 4 phases:

**Phase 1 (*CRSA model definition*):** The process starts with the definition of the cyber range security assurance (CRSA) model for an organisation, which defines: (1) the cyber-system(s) of the organisation that should be covered by the training (cyber-system sub model), (2) the security threats for these systems, the risks that these threats create and the security mechanisms that are used to mitigate these risks (cyber security assurance sub model), (3) models for assessing the likelihood and impact of risks (risk assessment sub model), and (4) models for threats and incidents that emerge as the system is being used (threats and incidents sub model).

**Phase 2 (Generation of Trainee Type Specific CRST programmes):** The next phase of the process is the generation of CRST programmes, tailored to the needs of different types of trainees within the organisation (e.g., security experts, end users, and stakeholders with responsibility for security investments). The generation of such programmes will be based on the CRSA model, which provides the specifications of system components, risks and the security mitigation mechanisms that will be targeted by the programme, as well as the risk and cost/benefit models available to evaluate the likelihood and impact of risks, and the costs/benefits of the security mechanisms.

**Phase 3 (Delivery of CRST programme):** The delivery of a CRST programme involves the emulation of the cyber-system components involved in the programme and the simulation of threat attacks to it. In this phase, trainees will be interacting with the cyber range platform of *AERAS* according to the training scenarios of the executed CRST programme. During the 3rd phase CRST programmes, all actions of trainees will be monitored (see **Continuous Performance Monitoring** in Figure 1), to assess their performance (e.g., the difficulty level they can reach within a training scenario, how many correct decisions they have made, whether their performance improves over time).

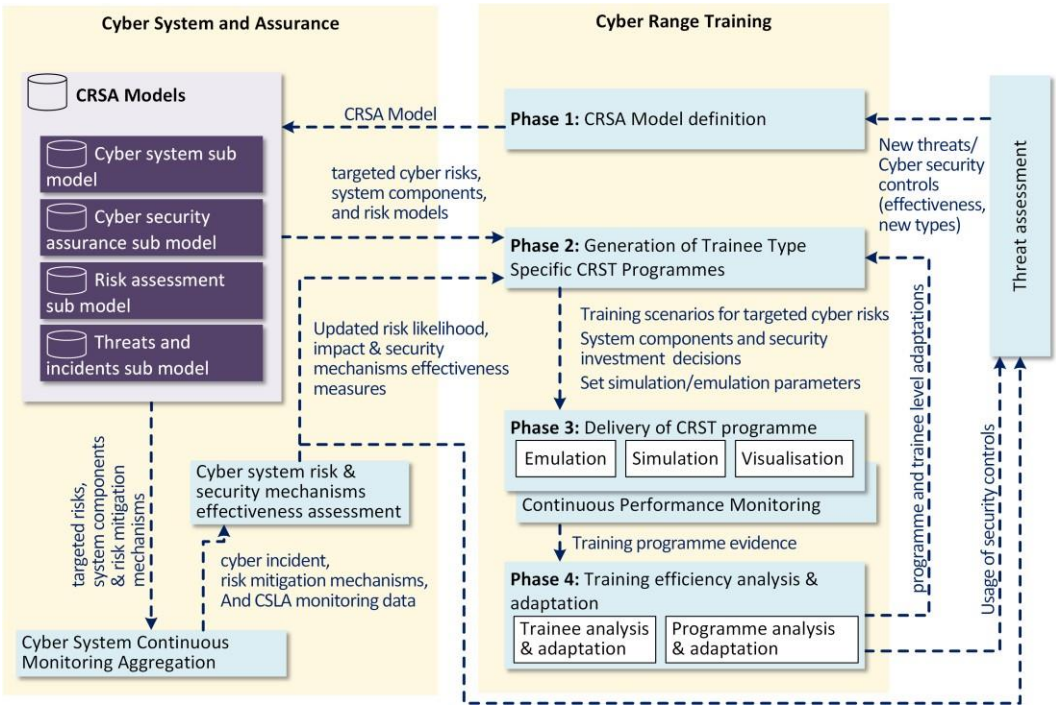


*Figure 1. General Cyber Range Simulation and Training Process.*

**Phase 4 (Training Efficiency Analysis and Adaptation):** Based on evidence collected during training (Phase 3), 4th phase of CRST process will identify deficiencies and gaps in the training programme and try to address them through CRST programme adaptation at either the individual trainee or the programme level. An example of possible adaptation at the former level is altering the configuration parameters of the programme in order to make it more or less challenging (e.g., to increase the attack rate and decrease the expected response time, to introduce multiple simultaneous attacks, to eliminate certain security controls or add more controls). Similar actions may be taken at the programme level, except that these would then become applicable to anyone who undertakes the programme next.

Two more activities will run in parallel with the execution of the main cyber range training process: (1) the **continuous multi-layer monitoring** of the cyber-system that is the focus of training, and (2) the **assessment** of the **actual risk** and the **effectiveness** of **security mechanisms** of it. These activities are important as they may trigger adaptations of training programmes. For example, they may provide more realistic information about threat rates (e.g., rate of intrusions at the network/server level), security controls performance (e.g., availability of authentication servers, effectiveness of anti-virus software) and real end-user actions. Such information can alter the simulations and emulations of the training programme, e.g., by providing more accurate values to parameters.

**Cyber range Security Assurance Models**

*AERAS* will delivers CRST programmes based on **Cyber Range Security Assurance (CRSA) models**, to ensure full alignment between the security assurance activities in an organisation and the cyber range training and simulation programmes. A CRSA model is an extended form of a security assurance model (i.e., a model used to specify the security requirements and controls of software systems and the processes of assessing them for the purposes of security audit and certification) that will be used to drive the generation of cyber range simulation and training. More specifically, a CRSA model will include four submodels:

- The **cyber system submodel** – This model is a specification of the cyber-system to be protected, which includes its software components, external services and devices, the computational and communication infrastructure used by it, and the organisational processes through which the system is used.
- The **cyber security assurance submodel** for the cyber-system – This submodel is a specification of the potential threats and attack scenarios assumed for the organisation, the risks that these threats and attacks create for different system assets and the security mechanisms available to combat the risk.
- The **risk assessment submodel** – This submodel specifies how to assess the probability of occurrence of the different types of risks specified in the assurance model.
- **Threats and incidents submodel** – This submodel specifies the bidirectional exchanges of information exist between the *AERAS* platform and received evidence about new threats and the effectiveness of security controls (e.g., from the results of training sessions or from monitoring security events on the actual cyber system).

**Model-driven Cyber Range Training Scenarios**

The purpose of cyber training in *AERAS* will be to help those with responsibility for security develop a systematic

understanding of: (1) possible manifestations of cyber-attacks and risks; (2) the impact of occurred and potential risks; (3) the effectiveness and the cost/benefit of the employed and alternative security (i.e., cyber risk mitigation) mechanisms for a risk; and (4) possible recovery actions, including actions necessary for exercising the established CSLAs to support recovery.

The generation and delivery of cyber range simulation and training (CRST) programmes will be driven by CRSA models. The starting point in generating such training programmes will be the **attack scenarios** specified in the cyber security assurance model. These scenarios will determine the threats and risks to be covered by the CRST programme and, subsequently, the **affected system assets** (e.g., compromise of a given system data store, denial of service attack on an emulated component) and the **security mechanisms** that are **available** and/or **used** to mitigate risks. CRSA models will provide the information needed to emulate or simulate the components involved in the scenario.

The CRST programme difficulty level will be determined by the **configuration options** specified for trainees with different roles in the attack scenario underpinning the programme. Such options will **regulate the types of information** regarding the attack that will be **available to trainees**, **when** this **information becomes available**, and the **level of detail** of the information generated from the cyber security systems. Depending on their role and expertise, trainees will be assessed at **different** and **adjustable levels of difficulty**, ranging from basic abilities (e.g. awareness of good computer practices and how to report incidents) to more advanced ones (e.g. trying to stop an active red team from hijacking systems or forensically investigating incidents). CRST programme exercises will feature a basic opening scenario that will be enriched with **injections**, i.e. new sets of information and/or events that progress the scenario. Injections may be generated by the CRST programme (s-injections) or users (u-injections). User-injections may be introduced by trainee or red team actions or manually by the cyber range instructor.

In many CRST programmes, the **trainees** will be **expected to interact with** the **emulated/simulated components** of the **cyber-system** during training. They will also be expected to monitor these components; observe the effects and propagation of various events and incidents; **identify and assess the effectiveness of the CSCs** used to mitigate the attack; **initiate or affect the behaviour** of some of these **CSCs** if relevant; and come to an **overall conclusion** on the **impact of the attack**, using the risk assessment methods of the risk assessment submodel. In some cases, the delivery of training will take the form of a "serious game", consisting of questions and challenges regarding appropriate responses to cyber-attacks. For example, a question could be who they can trust to handle devices (system administrators or other personnel?), how to assess the security status of the infrastructure assuming that the already deployed security measures are working properly, or who they should inform in case of erroneous or suspicious system functionality (e.g., corrupted or modified data, system hangs, etc.). An examples of a training scenario envisaged in *AERAS* appears in Table 1.

***Table 1: Indicative training scenario***

| |
|---|
| *The hospital receives an anonymous email containing EHR records of hundreds of patients, stating that the EHR records of thousands more of the hospital's patients have been acquired and will be sold to the highest bidder in the Darknet. Bids will close in 48 hours, and the sender asks for €100.000 to be paid via Bitcoin, in order to delete the obtained records. As a member of the Information Security team, you are urgently called to investigate the incident. The hospital is using a 3rd party Health Management software suite. Caregivers access the software via an internet facing webpage front end, while an SQL server runs at the back end. Examining the format of the leaked files, you suspect they originated from the specific database.* |
| **S-Injection 1:** An SQL event log of only two weeks is produced to give the trainee a hint of unauthorised access to data. **U- Injection 1:** You (the trainee) examine the SQL logs and see the partiality of it; **U-Injection 2:** You examine the front-end web page and discover that the clinical staff login name field does not perform data validation and allows SQL statements to be sent to the SQL server (SQL injections); **U-Injection 3:** Upon examining the SQL server you find a large file containing the patient EHR table stored on the root of the c: drive. This confirms the vulnerability that led to accessing the EHR records. |
| **Scenario modelling:** The **Cyber Security Assurance submodel** specifies EHR Leak as an **Attack Scenario** which generates **Cyber Threat** (SQL-injection) and subsequently a **Risk,** i.e., the violation of the **security properties** of confidentiality and privacy of EHR records (**Cyber System Asset)**. This cyber system asset depends on two other system components: the back- end database server (**Cyber System Asset)** and the system front end (**Cyber System Asset)** through which data can be inserted to and extracted from the database server. In this attack scenario, the **configuration parameters** set the front end not to check incoming data, thus allowing an attacker to gain access and manipulate database tables, or write and execute malicious scripts. |
| **Mitigation:** To *mitigate* the risks stemming from this scenario, appropriate **Security Mechanisms** have to be implemented. As the incoming data has to be validated at the **ASL** front end input function, there is a choice of **CSCs** that could be used. These include input validation/sanitization/canonicalization, or integrity checks [60][61][62]. **CSLA terms** and **policies** could also be set to cover part of the specific risk exposure (e.g. SLA coverage for this or similar threats in database back end provided by 3rd parties). Moreover, **CRST training** focused on software engineers and tailored to raise awareness for the specific type of vulnerability (input validation and secure software development practices) would help in the long-term mitigation of associated risks. In the CSAM, each of the above **Security Mechanisms** has **cost, benefit**, and **effectiveness** associated with it, and the trainee is tasked with deciding the optimal combination from a cost/benefit perspective. |

### 2.1.5 Overall research approach

#### The AERAS Platform

Figure 2 shows the envisaged high-level architecture of *AERAS* platform. The platform will include tools organized in three layers: the layers of assurance, cyber range and training tools. It will also has a vertical tools, i.e., the cyber- system continuous monitoring aggregator which is interfaced with the deployed environment (actual cyber system). A brief overview of the key components within this envisaged high-level architecture are presented below:

#### Assurance Tools

These are the core modelling and assessment tools of the platform. The **CRSA Model Editor** is responsible for the generation, adaptation and configuration of the CRSA models, used by *AERAS* for the generation of CRST programmes. The **Cyber-system Real-time Risk Evaluator**, in turn, will orchestrate the continuous cyber security risk assessment of the organisation, leveraging the *AERAS* hybrid cyber security risk analysis models, and produces the necessary information run-time evidence for the specification and adaptation of CRSA models (e.g., CRSA parameter values). Finally, the **Threat Assessor** is responsible for assessing how changes in the wider cyber security relate to and may affect the CRSA model of an organisation.

#### Cyber Range & Training Tools

The main role of the Cyber Range tools is to prepare the cyber range-based training through the generation of the associated programmes and the involved simulated and emulated elements, feeding the Training tools. The latter are the main components that deliver the training programme and evaluate the programme's performance. They include the **CRST Programme generator**, which uses CRSA models to setup the training environment (cyber-systems deployment, attack scenarios, available security measures, trainee roles and profiles, etc.). The training environment will mimic the cyber infrastructure of the organisation via the **Component Emulator** and **Cyber-system Simulator** too ls, based on the cyber-system submodel of CRSA. The **CRST Programme generator** will also consider the already deployed security mechanisms and their effectiveness, as defined in the cyber security assurance submodel and use them to drive the simulated attacks, thus, delivering adaptable training. During each training session, the Trainees will interact with the **Visualizer** component to deliver the attack scenarios and receive the information for identifying and responding to the simulated cyber-attacks. The **Trainee & Programme Performance Evaluator** will collect data on the CRST programmes and the behaviour of the trainees in terms of the effectiveness of their actions when faced with each attack scenario. The trainee and programme performance data will be fed back to the Cyber-System Real-time Risk Evaluator (via the Performance Monitor component of the Cyber-Systems Continuous Monitoring Aggregator), to adjust its risk estimations accordingly (e.g., by updating the parameters related to the effectiveness of the training security mechanism). Moreover, the **Programme Adaptor** tool will be used adapt CRSA models, and the associated CRST programmes, to enable their continuous improvement, based on aspects such as acquired security skills, completion percentage and completion time, deviation from results expected, etc.

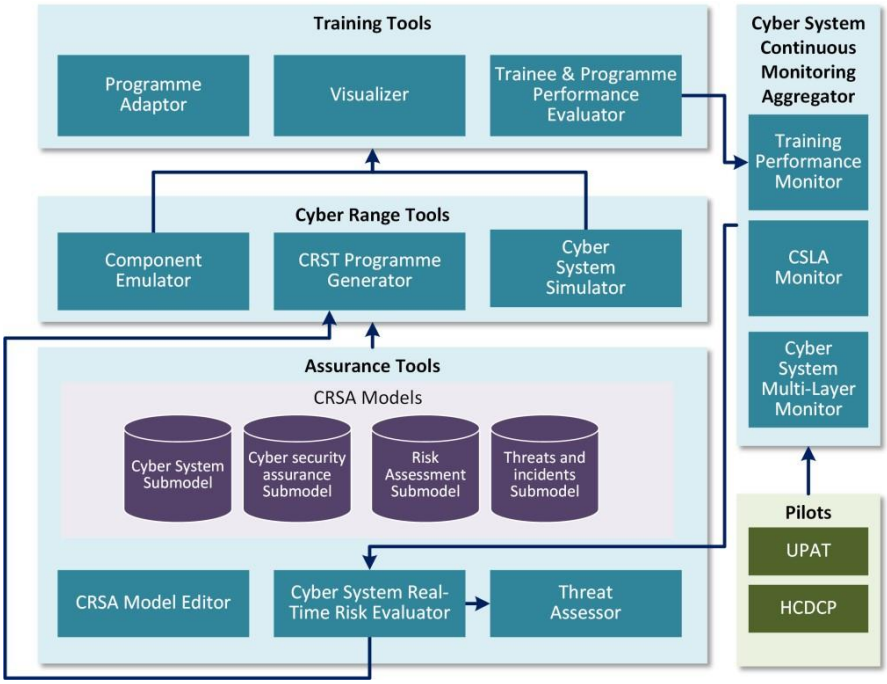


*Figure 2: Envisaged AERAS platform*

**Continuous Cyber-System Monitoring Aggregator**

The **Training Performance Monitor** will be collecting information on the performance of cyber range programmes and trainees; it will aggregate information on the performance of the *AERAS* CRST training, including the CRST programmes and the Trainee performance. These mechanisms will support assessments based on several inputs, including: (1) feedback on acquired security skills obtained from trainees and their supervisors, including contrasting security-related actions of trainees against the real cyber-system (e.g., compliance to security restrictions) prior to and after completing the training; (2) automatically recorded performance measures regarding the undertaking of the Cyber Range programme (e.g., programme completion time statistics, extent of programme completion statistics); (3) contrasting security related actions of trainees against the real cyber-system (e.g., compliance to security restrictions) prior to and after completing the training; and (4) assessing the level of compliance of these actions to expectations set by the security assurance sub-model of the CRSA model. The **Cyber-system Multi-Layer Monitor** will be responsible for the aggregation of cyber-system security monitoring information needed to assess the organisation's real-time security status, risk exposure and control performance/effectiveness. It will span across the layers of an organisation's cyber infrastructure, including end-points such as IT assets and the network; as well as applications (e.g. monitored through software security monitors), all in the context of the organisation's processes, and will consider end-user interactions and compliance to currently required regulations and certifications. Moreover, **CSLAs Monitors** will provide monitoring information regarding the compliance to the terms of active CSLAs (e.g. scope, positive/negative results, violations, relevant service request and response events).

**Targeted Pilot Cyber-systems**

*AERAS* will tailor its risk assessment and management, cyber range training, and validation activities to the NIS critical healthcare sector. To do so, it will use two pilots: (1) a hospital environment pilot, including various healthcare devices, and; (2) a healthcare authority pilot, interconnected (by nature of its role) with various public and private hospitals and individual healthcare professionals. These pilots have been selected as they involve: (i) heterogeneous types of system components, devices, networks and interactions, both within and across healthcare domains; (ii) different security and privacy cyber threats and requirements; and (iii) different types of actors who need to be trained. Due to their variabilities, the pilots provide scope for broad coverage of technical, business and regulatory issues which should be accounted for in developing the *AERAS* platform. Thus, they will drive the innovation work of the programme effectively, and allow for a comprehensive demonstration and evaluation of its outcomes.

When validating the pilots, the focus will be to assess whether the cyber range training has an effect on the behaviour and effectiveness of different types of healthcare staff over security issues. These will be: (a) clinicians using the medical systems in their daily clinical practice; (b) technical hospital staff responsible for maintaining and administering the medical and cyber-systems, including cyber security professionals; (c) staff involved in healthcare organisational processes who must use the systems employed in the pilots; and (d) hospital staff responsible for cybersecurity SLAs with external parties. The effectiveness will be measured in terms of: (a) improvements in performance; (b) any notable effects on cyber threats experienced by the organisation; and (c) the effect onto clinical practice of staff actions addressing security issues (e.g., how false alarms may affect what clinicians do; how shutting down or disconnecting devices and servers to contain a cyber-attack affects the clinical services provision). The main features of the pilots are summarized below.

**Hospital Environment Pilot (UPAT)**

**Description:** The University of Patras, School of Medicine has a daily presence in the University Hospital of Patras, where each Department has a clinical unit. To this end all the faculty of the school of medicine are members of the University Hospital staff and do their daily clinical routine in the corresponding clinical units. The hospital environment has image acquisition units like the PET/CT, CTs, SPECT/CTs, MRI, mammography units, Diagnostic RX units, various laboratory tests, liquid biopsies, etc. Every patient is subjected to various tests during his/her stay in the hospital and their data are archived in various DBs. Data are transferred through the various members of the personnel during every patient's stay in the hospital.

**Security and Privacy requirements and threats:** processes health data containing highly personal information. There are numerous data that are archived every day since there are about 1,000 patients every day examined in the hospital. Those data are of high importance and need be protected against any illegal action. Systems acquiring data, as well as archiving and transferring them need be operable on a 24/7 basis.

**Foreseen stakeholders (direct/indirect) involved in the pilot scenarios:** End-users (medical doctors, nurses, administrative personnel, biochemists, etc.) who interact with the various DBs, and systems; patients who want to access the results of their examinations, systems who interconnect to each other in order to transfer data, i.e. PACS server with image acquisition units.

**General significance and impact potential of the pilot:** Because of the nature of the information i.e. patient data, it's

critical that those data are not lost, stolen, manipulated, and reach their destination at real time. It's critical that data are calibrated among various machines producing the same type of data and reach their final destination on time.

**Healthcare Authority Pilot (PAGNI)**

**Description:** "Platforms of healthcare authorities interconnected with hospitals and healthcare professionals"

PAGNI uses an integrated information system, called OPSI, that offers the following administrative and clinical services: Medical-nursing services (HIS); Administrative-economic services (ERP); Laboratory services (LIS); Medical Imaging services (RIS/PACS); Intensive treatment unit services (Critis); Technical biomedical services (MASO/POINT).

**Security and Privacy requirements and threats:** PAGNI processes health data containing highly personal information, so it is a prime target for cyber-attacks whose goal is to obtain such information unlawfully. At the same time, a disruption of its systems and their unavailability due to viruses/ransomware will affect many others – both those who attempt to provide up-to-date information on the various topics it is monitoring, and the partners connected to it. PAGNI is connected to 7 other hospitals located in Crete, general practitioners, public health centres, the University of Crete and the 7th Health Region of Crete.

**Foreseen stakeholders (direct/indirect) involved in the pilot scenarios:** End-users (health professionals with no specific security or privacy knowledge) who interact with PAGNI systems; and PAGNI's ICT personnel with specialties in in-house development and the administration of e-health systems, personnel with expertise in developing public health policy.

**General significance and impact potential of the pilot:** The general significance of this pilot derives from the fact that PAGNI is the largest hospital facility in Crete and one of the largest public hospitals in the country, with 760 beds, more than 2000 employees and 8.200 surgeries per year. The estimated annually hospitalised patients amount to 83.500, while the visits to the Emergency and Outpatient Department ranges from 100.000 to 130.000 per year. As a result, it is crucial for PAGNI to maintain the confidentiality and integrity of its data but also the availability of its services.

### 2.1.6 Interdisciplinary nature

*AERAS* is a research and innovation programme involving knowledge at the junction of two generic scientific disciplines, i.e., computer science, and healthcare and its applications. It also involves cross-cutting knowledge from the field of *risk assessment*, with different manifestations: *security risk assessment in (a)* cyber system asset, vulnerabilities, threat and risk modelling and evaluation, and *risk assessment in (b)* assessment of risks for different types of assets under SLAs. AERAS aims to make specific advancements to the state of the art in all the fields related to its research and innovation programme (i.e., security certification, risk assessment and CSLAs – cf. Sect. 2.1.3). Driven by its overall aim to carry out an interdisciplinary investigation, *AERAS* has formed a consortium of industrial organisations and universities with complementary expertise in them and their wider disciplines. These types of expertise and their complementarity are discussed in Sect. 2.3 below, along with other areas of knowledge within (a) and (b) that are required for the successful completion of *AERAS*.

### 2.1.7 Gender aspects

*AERAS* has formed a consortium and a programme of work that is in line with the EU policy on equal opportunities for different genders. More specifically, the *AERAS* consortium includes comparable numbers of male and female secondees (19 male and 7 female) both at the level of individual partners and at the level of the consortium as a whole. Gender balancing is present in research, and five of the seven partners involve experienced female researchers, who may undertake administrative roles in hosting and partner representation in the *AERAS* management structure (e.g., WP leadership, representation in GA etc.). The organisation of all project activities will be carried out in a manner that is aware of family and parenting commitments of female researchers. Gender aspects are considered both at the level of secondments and that of decision-making within the project.

## 2.2 Quality and appropriateness of knowledge sharing among the participating organisations in light of the research and innovation objectives

The knowledge sharing, which is required for carrying out the inter-disciplinary investigations that are necessary for the successful achievement of the objectives of AERAS, will be realised through the plan of secondments that is presented in Table B2.2.1 below. This plan is based on the expertise of the different partners of AERAS at an institutional level and the expertise of the individual researchers who will participate in the secondment. The former sort of expertise provides the basis for the knowledge transfer described under the column "Knowledge Gained … during Secondment" of Table B2.2.1. The latter type of expertise provides the basis for the knowledge transfer described under the column "Knowledge Transfer … during Secondment" of Table B2.2.1. The collective expertise of different partners and of their individual researchers that is relevant to the knowledge transfers described in Table

B2.2.1 are described in Sect 2.3.1.

**Table B.2.2.1: Transfer of knowledge per fellow/secondment/Work Package**

| ID | From | To | WP | Knowledge Transferred from Fellow to Hosting Institution | Knowledge Gained by Fellow from Hosting Institution |
|---|---|---|---|---|---|
| 1/ER | UMIL | STS | 2 | Security control, risk analysis, cyber range requirements, esp. for edge/cloud security. Design and deployment of secure systems. | Security assurance, security certification, and cyber range requirements. |
| | | AEGIS | 4 | Security control, risk analysis, cyber range requirements, esp. for edge/cloud security. Design and deployment of secure systems. | Cyber range tools, adaptive visualization, tools for digital forensics investigations and emulation/simulation. |
| | | PAGNI | 4 | Security control, risk analysis, cyber range requirements, esp. for edge/cloud security. Design and deployment of secure systems. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| 2/ER | | PAGNI | 3 | Emulation, Analytics and their support by the AERAS CRSA language and CRSA models, esp. for the analysis of risks. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | AEGIS | 3 | Emulation, Analytics and their support by the AERAS CRSA language and CRSA models, esp. for the analysis of risks. | Cyber range tools, adaptive visualization, tools for digital forensics investigations and emulation/simulation, and how the CRSA language can support these. |
| | | STS | 5 | Emulation, Analytics and how to evaluate these within the framework of the AERAS platform and pilots. | Evaluation methods for Security assurance, security certification, and cyber range. |
| 3/ER | | AEGIS | 3 | Security Assurance, Modelling – applied to security properties and the features that the CRSA language will need to include in order to support these. | Cyber range tools, adaptive visualization, digital forensics investigations and emulation/simulation. Secure embedded and privacy preserving systems properties. |
| | | PAGNI | 4 | Security Assurance, Modelling – simulation and real- time cyber security assurance models. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | STS | 3 | Security Assurance, Modelling – applied to security properties and the features that the CRSA language will need to include in order to support these. | Properties usually supported by security monitoring and testing in industry, intrusion detection and fraud management identification methods. |
| 4/ESR | | STS | 4 | Cyberagents Training, Security Framework; blockchains and their use in security assurance. | Security monitoring, intrusion detection, and fraud management – frameworks for these. Cyber range training systems. |
| | | PAGNI | 5 | Cyberagents Training, Security Framework; methods and techniques for their evaluation. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | AEGIS | 5 | Cyberagents Training, Security Framework; blockchains and their use in secure decentralised applications. | Secure embedded platforms and privacy preserving systems. |
| 5/ER | CITY | STS | 2 | SLAs, Security Assurance and modelling, formal methods – formal modelling/analysis of systems and their requirements. | Methods for monitoring threats and performing security audits and certification. |
| | | AEGIS | 4 | SLAs, Security Assurance and modelling; real-time assurance & CSLA monitoring. | Access control and network security systems, privacy preserving systems. |
| | | PAGNI | 5 | SLAs, Security Assurance and modelling; evaluation of security assurance and CSLA monitoring. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| 6/ER | | AEGIS | 4 | Security modelling/Certification, SLAs, Cyber Range; cyber sec. assurance models & CSLA monitoring. | Cyber range tools, adaptive visualization, tools for digital forensics investigations and emulation/simulation. |
| | | PAGNI | 5 | Security modelling and Certification, SLAs, Cyber Range; evaluation of security assurance & CSLA monitoring. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | STS | 5 | Security modelling and Certification, SLAs, Cyber Range; formal evaluation methods. | Evaluation methods for Security assurance, security certification, and cyber range. |
| 7/ER | | STS | 3 | Security Controls and Assurance, Big Data, advanced methods for penetration testing. | Properties usually supported by security monitoring and testing in industry, intrusion detection and fraud management identification methods. |
| | | AEGIS | 3 | Security Controls and Assurance, Big Data, advanced methods for penetration testing. | Cyber range tools, adaptive visualization, tools for digital forensics investigations and emulation/simulation. Secure embedded and privacy preserving systems properties. |
| | | PAGNI | 4 | Security Controls and Assurance, Big Data, advanced methods for penetration testing. | Healthcare authority processes and systems, collaborations in public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | STS | 4 | Security Controls, Assurance, information security methods. | Security monitoring, intrusion detection, and fraud management – frameworks. Cyber range training systems. |

| | | | | | |
|---|---|---|---|---|---|
| 8/E | | PAGNI | 3 | Security Controls, Assurance; system analysis methods for security. | Healthcare authority processes and systems, collaborations in public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | AEGIS | 4 | Security Controls, Assurance, information security techniques. | Secure embedded and privacy preserving systems; tools for forensics investigations and emulation/simulation. |
| 9/ER | CUT | PAGNI | 2 | Analyzing (and building) trust in distributed systems. Social networks and security/privacy issues in them. Identity management. | Healthcare authority processes and systems, intersectoral collaborations during public health threats/emergencies; how these are supported technically, systems/methods used for training staff. |
| | | AEGIS | 4 | Trust management in decentralised systems; Identity management. | Secure embedded and privacy preserving systems; tools for forensics investigations and emulation/simulation. |
| | | STS | 5 | Trust & Identity management methods and evaluation of these in systems. | Security monitoring, intrusion detection, and fraud management – frameworks for these. Cyber range training systems. |
| 10/ER | | STS | 3 | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. | Cyber range security assurance concepts and methods. |
| | | AEGIS | 4 | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. | Simulation and visualization methods and tools. |
| | | PAGNI | 5 | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. | Systems/methods used for training staff on health threats/emergencies. |
| 11/ER | | STS | 3 | Cyber Range Training tools; formative and peer-assessment methods. | Cyber range security assurance concepts and methods. |
| | | AEGIS | 5 | Cyber Range Training tools; formative and peer-assessment methods. | Evaluation of simulation and visualization methods and tools. |
| | | PAGNI | 4 | Cyber Range Training tools; formative and peer-assessment methods. | Systems/methods used for training staff on health threats/emergencies. |
| 12/ESR | | STS | 3 | Security Controls and Simulation; identity management & analysis of social networks. | Security monitoring, intrusion detection, and fraud management – frameworks for these. Cyber range training systems. |
| | | PAGNI | 4 | Security Controls and Simulation; authentication security, identity management, social network analysis. | Healthcare authority processes and systems, collaborations during public health threats/emergencies; how these are supported technically, systems/methods for training staff. |
| | | AEGIS | 3 | Security Controls and Simulation; social network analysis. | Cyber range tools, visualization, tools for digital forensics investigations and emulation/simulation. Properties of secure embedded and privacy preserving systems. |
| 13/ER | STS | CITY | 2 | Security Assurance and risk analysis for smart ecosystems and their requirements. | SLAs, Security Assurance and modelling, formal methods – modelling/analysis of systems and their requirements. |
| | | UMIL | 3 | Security assurance and risk analysis concepts and their categorization – help with developing the CRSA language. | Security Assurance, Modelling – applied to security properties and the features that the CRSA language will need to support these. |
| | | CUT | 4 | Security monitoring, intrusion detection, and fraud management – frameworks for these. | Security Controls and Simulation; identity management & analysis of social networks. |
| 14/ER | | UPAT | 2 | Biomedical system security, training environments; requirements for secure healthcare systems. | Healthcare services and processes; needs of different stakeholders. |
| | | CITY | 3 | Biomedical system security, training environments; concepts requiring support from CRSA. | Methods for analyzing security requirements; simulation concepts. |
| | | UMIL | 3 | Biomedical system security, training environments; concepts requiring support from CRSA. | Cyberagents Training, Security Framework; Emulation concepts. |
| 15/ER | | CUT | 4 | Security and privacy, risk analysis, inclusive design for visualization and cyber range training systems. | Simulation and visualization methods and tools. |
| | | CITY | 5 | Security and privacy and inclusive design evaluation. | Security modelling and Certification, SLAs, Cyber Range; formal evaluation methods. |
| | | UPAT | 5 | Security and privacy and inclusive design evaluation. | Systems/methods used for training staff on health threats/emergencies. |
| 16/ESR | | UMIL | 4 | Cyber range training systems. | Cyberagents Training, Security Framework; blockchains and their use in security assurance. |
| | | CUT | 4 | Cyber range training systems. | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. |
| | | UPAT | 3 | Cyber range training systems. | Systems/methods used for the secure exchange of information within a healthcare provider. |
| 17/ER | | UPAT | 2 | Cyber Range Training, Security Assessment; requirements analysis, digital forensics. | Systems/methods used for the secure exchange of information within a healthcare provider; requirements of different stakeholders. |
| | | CITY | 4 | Cyber Range Training, Security Assessment; digital forensics guidelines. | Security modelling and Certification, SLAs, Cyber Range; real-time cyber security assurance models & CSLA monitoring. |
| | | UMIL | 4 | Visualization, User interfaces, Analytics | Cyber range tools, adaptive visualization, tools for digital forensics investigations and emulation/simulation. |

| | | | | | |
|---|---|---|---|---|---|
| 18/ER | AEGIS | UPAT | 4 | Cyber Range Training, Security Assessment; digital forensics guidelines. | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. |
| | | UPAT | 5 | Visualization, User interfaces; evaluation of the cyber range system. | Systems/methods used for training staff on health threats/emergencies. |
| | | CUT | 5 | Visualization, User interfaces; evaluation of the cyber range system. | Cyber Range Training and tools; formative and peer-reviewed assessment methods. |
| 19/ESR | | CITY | 3 | Visualization, User interfaces | Security Controls and Assurance, Big Data, advanced methods for penetration testing. |
| | | UMIL | 3 | Visualization, User interfaces | Emulation, analytics and their support by the AERAS CRSA language and CRSA models, esp. for risk analysis. |
| | | UPAT | 5 | Visualization, User interfaces | Systems/methods used for training staff on threats/emergencies. |
| 20/ER | PAGNI | UMIL | 2 | National health policy, European standards compliance, emergency responses: requirements. | Security assurance, analysis, cyber range requirements |
| | | CITY | 3 | National health policy, EU standards compliance, emergency responses systems and processes. | Security modelling and Certification, SLAs, Cyber Range; evaluation of security assurance & CSLA monitoring. |
| | | CUT | 4 | National health policy, EU standards compliance, emergency responses systems and processes. | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. |
| 21/ER | | CITY | 2 | Healthcare authority processes and systems, collaborations in public health threats/emergencies. | SLAs, Security Assurance and modelling |
| | | UMIL | 4 | Healthcare authority processes and systems, collaborations in public health threats/emergencies. | Security assurance, risk analysis, cyber range |
| | | CUT | 4 | Healthcare authority processes and systems, collaborations in public health threats/emergencies. | Cyber Range Training tools and simulation; innovative educational technologies and learning environments. |
| 22/ESR | | UMIL | 4 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Simulation and real-time cyber security assurance models |
| | | CITY | 4 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Security Controls and Assurance, Big Data, advanced methods for penetration testing. |
| | | CUT | 3 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Cyber Range Training tools; formative peer-reviewed assessment methods |
| 23/ESR | | CUT | 5 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Cyber Range Training tools and simulation; innovative educational technologies and learning environments |
| | | UMIL | 3 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Emulation, Analytics and their support by the AERAS CRSA language and CRSA models, esp. for the analysis of risks. |
| | | CITY | 5 | Healthcare authority processes/systems, collaborations during public health threats; how these are supported technically, systems/methods used for training staff. | Security modelling and Certification, SLAs, Cyber Range; evaluation of security assurance & CSLA monitoring |
| 24/ER | UPAT | STS | 2 | Medical Informatics, Healthcare applications. | Biomedical system security, training environments; requirements for secure healthcare systems. |
| | | AEGIS | 3 | Medical Informatics, Healthcare applications | Cyber Range Training, Security Assessment; requirements analysis, digital forensics. |
| | | STS | 4 | Medical Informatics, Healthcare applications | Cyber Range Training, Security Assessment; simulation. |
| 25/ER | | AEGIS | 3 | Medical application, Health Cloud computing | Cyber Range Training, Security Assessment; requirements analysis, digital forensics. |
| | | AEGIS | 5 | Medical application, Health Cloud computing | Visualization, User interfaces; evaluation of the cyber range system. |
| | | STS | 4 | Medical application, Health Cloud computing | Cyber Range Training, Security Assessment; simulation. |
| 26/ER | | STS | 3 | Health Technology Assessment, Medical Informatics Applications | Biomedical system security, training environments; concepts requiring support from CRSA. |
| | | STS | 3 | Health Technology Assessment, Medical Informatics Applications | Cyber range training systems. |
| | | AEGIS | 5 | Health Technology Assessment, Medical Informatics Applications | Visualization, User interfaces; evaluation of the cyber range system. |

## 2.3 Quality of the proposed interaction between the participating organisations

### 2.3.1 Contribution of each participant in the activities planned

Addressing the objectives of *AERAS* and making progress beyond the state-of-the-art research described in Sect. 2.1.3, requires knowledge in some key areas of expertise, while achieving the objectives of *AERAS* requires also expertise in some further enabling areas, such as healthcare services and applications, visualisation, simulation and emulation environments, as well as system integration and testing. Table B.2.3.1 demonstrates the current expertise and complementarity of all six partners of the *AERAS* consortium.

**Table B2.3.1: Key areas of partner expertise for AERAS objectives & work packages**

| Key Areas of Needed Expertise | UMIL | CITY | CUT | STS | AEGIS | PAGNI | UPAT |
|---|---|---|---|---|---|---|---|
| Visualisation | | | | | ● | | |
| Security Assurance & Modelling | ● | ● | | ● | | | |
| Security Controls | ● | ● | ● | | | | |
| Risk Analysis | ● | | | ● | | | |
| Service Level Agreements | | ● | | | | | |
| Healthcare Services and Applications | | | | | | ● | ● |
| Cyber Range Training | ● | ● | ● | ● | ● | | |
| Simulation Environments | | | ● | | | | |
| Emulation Environments | ● | | | | | | |
| System Integration & Testing | ● | | | ● | ● | | |

Beyond the knowledge and expertise that individual partners bring to the *AERAS* consortium in order to achieve the project's objectives, *AERAS* is expected to generate new knowledge and make advancements to the state of the art in several key areas (cf. Sect. 2.3.1). These will enhance the expertise of all partners in specific areas. Table B2.3.2 shows the key areas of progress beyond the state-of-the-art that we envisage to make in *AERAS* and how the respective *AERAS* partner will contribute to and benefit from it. The table identifies the partners that will have an active role in creating new knowledge in a specific area (shown by "§") and those who will enrich their knowledge base and expertise through the advancements made by AERAS (shown by "+"). As shown in Table B2.3.2, AERAS will broaden the range of expertise of all partners and enable cross-sector and cross-discipline knowledge sharing. The active role of all partners in making advancements in at least two areas of knowledge and the interest of all partners in enhancing their knowledge in all key areas demonstrates the added value that the project can bring to the partners.

**Table B2.3.2: Partner Involvement in the Generation of New Knowledge & State-of-the-Art advancement by AERAS**

| New Knowledge and Advancement Area | UMIL | CITY | CUT | STS | AEGIS | PAGNI | UPAT |
|---|---|---|---|---|---|---|---|
| Visualisation | | + | | + | § | | |
| Security Assurance & Modelling | § | § | + | § | + | + | + |
| Security Controls | § | § | § | + | | | |
| Risk Analysis | § | + | | § | + | | |
| Service Level Agreements | + | § | + | + | + | + | + |
| Healthcare Applications | | | | | + | § | § |
| Cyber Range Training | § | § | § | § | § | + | + |
| Simulation Environments | + | + | § | | | + | + |
| Emulation Environments | § | + | | + | | + | + |

### 2.3.2. Justification of networking activities

The different partners of the *AERAS* consortium have complementary expertise in areas that are necessary for conducting the research & innovation programme of *AERAS* and achieving its general objectives, as shown in Table B2.3.1. Furthermore, we have devised a clear programme of knowledge sharing and intra-consortium networking activities, which involves (a) researcher exchanges (secondments), (b) structured knowledge transfer activities (e.g., seminars), (c) other internal training activities, and (d) networking beyond the boundaries of the *AERAS* consortium.

The exact purpose, plan and knowledge sharing of (a) to (d) has been described in detail in Sect. 2.2 above. This information provides a clear justification of the role and the necessity of all the networking activities of *AERAS*.

## 3. Impact

### 3.1. Enhancing the potential and future career perspectives of the staff members

AERAS forms a multi-disciplinary group of researchers and practitioners from industry and academia, who will participate in exchanges that will enable them to work collaboratively, and to transfer and gain the different types of multi-disciplinary knowledge that is necessary in order to develop a holistic solution to the targeted problem. The staff participating in AERAS's programme of secondments will get in-depth knowledge and hands-on experience in research and innovation from hosting partners with long standing experience in different areas of the project. Moreover, they will be given the opportunity to work with 13 experienced researchers in academic institutions and 7 experienced industry staff in the specialised enterprises of the consortium, collectively bringing expertise in cyber range training, emulation and simulation environments, security controls, security assurance, security SLAs, visualization, healthcare services and applications, and system integration. The exchanges have been designed to complement and consolidate the existing knowledge, skills and experience of the involved staff in the areas of cyber range training,

emulation/simulation environments, security SLAs and security assurance. This will make them more competitive and enhance their career prospects in the longer term both within and outside their existing organisations. More specifically, the exchanged staff is expected to gain the following immediate and/or long-term benefits: (i) gaining experience and practical skills in cyber range training cutting edge models, techniques, methods and security control technologies, mechanisms, and tools, including – but not limited to – those that will be developed/integrated by AERAS itself; (ii) gaining experience in conducting collaborative research within a network involving industry and academia and covering several research areas and prior experiences (see table B2.3.1); (iii) gaining experience in research methodologies appropriate for the subject areas of the project; (iv) gaining experience in documenting and publishing research outcomes in high quality ways appropriate for addressing the research and industrial community, and/or other relevant stakeholders, (iv) gaining access to funding for participation in training events, conferences, (v) gaining access to a well-structured secondment enabling the exchange of knowledge between staff of different expertise areas and experience levels (see Table B2.2.1) and (vi) gaining the opportunity to work with research and industrial entities from different countries and with different cultural profiles that is regarded as a key career development prerequisite.

AERAS will also advocate a structured approach to career development of the fellows participating in it by establishing and monitoring a Personal Career Development Plan (PCDP). The PCDP will define: (a) the overall technical and business objectives, (b) the expected knowledge gains, and (c) the training that each fellow should receive for each of the secondments that they will participate. PCDPs will be personalised for the particular fellow and help them build a record and monitor the portfolio of skills gained through their participation in AERAS. It will also help the individual organisations to monitor their gains at an aggregate level, and the project as a whole.

## 3.2. Developing new and lasting research collaborations, achieving transfer of knowledge between participating organisations and contribution to improving research and innovation potential at the European and global levels

### 3.2.1. New and lasting research collaborations

All the *AERAS* partners are committed to a long-term research programme in the area of cyber security management and pertinent cyber range training, especially in the critical healthcare sector. This is due to the strategic importance of this area from a research, technology and business innovation perspective for all partners. At the outset, we expect long-term strategic collaborations to arise between partners in a number of key areas, such as cyber security assessment and security software development (UMIL, CITY, STS, AEGIS), cyber range training (UMIL, CITY, CUT, STS, AEGIS), tackling the intricacies of cyber security for healthcare environments (CITY, STS, PAGNI, UPAT), and model-driven simulation and emulation environments (UMIL, CITY, STS, AEGIS). The above research collaborations are expected to be of different forms:

**Visiting research positions:** The academic/research partners (UMIL, CITY, CUT and UPAT) have internal funding for visiting researchers and offer them, following approval by the appropriate organisational bodies, to the Principal Investigators (PI) of other consortium partners during and after the project, to explore long-term synergies.

**Promote the participation of the SMEs in future EU and National R&D programmes:** The academic partners have a long standing track record in EU and national R&D funding and seek actively to develop joint further research grant proposals with the two SMEs of the consortium, as well as the healthcare end user who have less experience in this, in the strategic areas of collaboration, such as those mentioned above.

**Bilateral self-funded projects between industrial and academic partners:** The interaction between the academic and the industrial partners within *AERAS* will strengthen their bonds and, subject to identification of mutually interesting opportunities, will lead to bilateral research and innovation projects. These can be self-funded projects by the relevant parties and/or projects funded by the industrial partners. The academic partners have prior experience and existing frameworks for administering such projects

### 3.2.2. Self-sustainability of the partnership after the end of the project

The potential for business and economic impact from the successful development of the *AERAS* framework is significant. To this end, the partners of *AERAS* will seek actively to find routes of joint potential exploitation of the project's framework or individual components of it depending on opportunities arising in specific markets. Potential instruments that will be used for this purpose include:

**Joint patent applications:** The technical partners of *AERAS* consortium will seek to develop and submit joint patent applications in the areas of cyber security assurance assessment, cyber range training and assessment, to safeguard the commercial exploitation of project outcomes and/or attract external financial support for the full commercial exploitation of the *AERAS* framework. Our view is that joint patents are important for having a self-sustainable collaboration beyond the duration of the project and can improve the innovation potential of *AERAS* in line with EU

strategies (e.g., Innovation Union [66]).

**Creation of Spin-offs:** Research-Based Spin-Offs (RBSOs) are seen as a potential mechanism for technology transfer by commercialising academic research and thereby stimulate industrial innovation. RBSOs can play an important role as technology transfer agents by converting scientific knowledge and inventions into new innovative products and services in the marketplace. *AERAS* partners will explore the possibilities for commercialising project outcomes through the creation of a new joint spin-off company or a spin off involving a subset of the interested consortium partners subject to the IPR over the outcomes that this entity will seek to exploit commercially.

In addition to the above possibilities, *AERAS* partners will seek to establish joint PhD and Continuing Professional Development (CPD) programmes in the scientific and technology areas of the project to enable the training of members (staff, researchers, students) of the partners beyond the duration of *AERAS*. For this, the consortium will develop a Memorandum of Understanding within the first year of the project.

### 3.2.3. Improving research and innovation potential within Europe and worldwide

Several reasons support the idea that the *AERAS* project is of great value for the European Community and will strengthen the European Research Area (ERA). It is a multidisciplinary and intrasectoral project which aims to bridge the gap between experimental cyber security, staff training and awareness, and the critical healthcare sector. Certainly, the validation of such approach will encourage other research groups to establish similar collaborations. The proposed project also represents an opportunity for EU through this integration grant, to support a consortium of academic and industry partners with innovative ideas aiming to join their strength to offer an appropriate solution to the management of cyber security risks in the sensitive healthcare sector Moreover, AERAS will introduce disruptive innovation related to cyber security awareness training within healthcare organisations, in the form of innovative cyber risk detection, response methods, and integrated tool-based cyber range training solutions. Healthcare organisations are characterised by the lack of use of State-of-the-Art cyber risk detection, response and costing methods, and integrated tool-based cyber range training solutions. In May 2017 WannaCry cyber-attack [69] affected the NHS cyber infrastructure by infecting several machines, resulting to a large part of the infrastructure going offline and several services (e.g., surgeries, appointments) being disrupted. According to the "SecurityScorecard 2018 Healthcare Report: A Pulse on The Healthcare Industry's Cybersecurity Risks" report, healthcare industry ranks 15$^{th}$ in cyber security preparedness when compared to 17 other major industries, while it is one of the lowest performing industries in terms of endpoint security, posing a threat to patient data and potentially patient lives. *AERAS* will develop an innovative platform due to the novelty of the holistic approach that it undertakes and the risk models that it will use in security training, its capability to cover new security risks, and adjust its CRST programmes and the introduction of a “security culture” in organisations.

IBM Security’s 2018 Cost of a Data Breach Study (a survey of more than 2,200 IT, data, protection and compliance professionals from 477 companies in 15 countries in the healthcare domain) calculated the costs associated with “mega breaches” ranging from 1M to 50M records lost, projecting that these breaches cost companies between $40M and $350M respectively. AERAS will reduce the impact and cost of cyberattacks in healthcare by enabling organisations to use not only effective internal security mechanisms (i.e., CSC, cyber security training) but also effective external security mechanisms (i.e., CSLAs). The former will reduce the occurrence rate/significance of successful cyberattacks, and the latter will provide more coverage of the resulting costs. The significance of these two effects in a healthcare organisation will be magnified by the significant costs that are linked to (a) delays in the provision of healthcare due to reliance on systems, devices and data that may become unavailable as a result of cyberattacks, and (b) the need to compensate patients and other third-party organisations due to loss of private or corporate medical data. Increasing the resilience of healthcare organisations to cyberattacks will also arise from improving the awareness and skills of healthcare organisation's personnel in detecting and managing cyber risks.

The proliferation of polymorphic attack vectors afflicts healthcare at higher rates than other verticals: FortiGuard Labs [70] reports that in 2017 healthcare saw about 32K/day intrusion attacks on average per organization, compared to over 14.3K in other industries. AERAS will improve the cost to benefit (CTB) ratio of using cyber security risk mitigation solutions in healthcare organisations by (a) the collection and analysis provision of operational evidence regarding cyberattacks and their effect on the assets of healthcare organisations, and the effectiveness of the security measures that are used against them (i.e., CSCs, CRSTs, and CSLAs); (b) the development of CRST programmes that will enable key stakeholders of healthcare organisations to be more vigilant against and identify cyberattacks, understand the operation of the employed security mechanisms, how to best interact with them when this is required; and (c) how to make effective decisions regarding investments in such security mechanisms.

Finally, AERAS will also increase the penetration of the cybersecurity products and services, including CSLAs, in the healthcare sector and beyond it. Healthcare, as a global industry, is expected to reach $2.69 trillion by 2025, according to Frost & Sullivan [63], while the National Journal expects employment in this sector to grow by 17.4% by 2024 clearly exceeding many other sectors [64]. Moreover, the global **digital** health market is projected to grow at a

compound annual growth rate (CAGR) in excess of 18% during 2018-2022 [65]. By increasing the awareness and skills of healthcare organisation stakeholders in detecting and managing cyber risks, the *AERAS* solution will help stakeholders realise the need for acquiring cyber security risk mitigation products and services (including CSCs, CRSTs, and CSLAs), and make effective use of such products and services in the context of their hectic daily clinical activities, thus reducing cultural barriers towards their adoption.

Moreover, the potential of this impact beyond the healthcare sector will be investigated by an analysis of the transferability of the *AERAS* approach and implemented solutions to other critical sectors (e.g., defence, transport). The evaluation of this potential will be integrated in the validation of the platform (documented in D5.6).

## 3.3. Quality of the proposed measures to exploit and disseminate the project results

### 3.3.1. Dissemination strategy

*AERAS* targets different types of stakeholders for disseminating project outcomes. These include direct potential users of the project outcomes, (a) healthcare CTOs, (b) cyber system providers, (c) educators and trainers (who can embrace and develop further the cyber-range platform of the project), and (d) the scientific and research community (consumers of outcomes for research purposes). It also includes other stakeholders, who may have an indirect interest in the AERAS outcomes, like (e) cyber system user groups, (f) policy makers (primarily in Europe), and (g) the general public. The dissemination strategy in this section concerns stakeholders (a)-(d), while groups (e)-(g) are covered by communication activities (see Sect. 3.4 below). The communication channels that will be used to realise its dissemination strategy for groups (a)-(d) are:

**(i) Direct interactive dissemination:** AERAS outcomes will be presented in: (a) industrial fairs, workshops and symposia; (b) networking events (e.g., events organised by the EU to coordinate projects in specific thematic, technology and business areas); and (c) scientific conferences, workshops and symposia. Direct presence of AERAS partners to such events will offer a chance for personal interaction with external stakeholders. It is also effective in providing information that is tailored to different target groups. The direct interactive channel of dissemination is expected to be the most efficient channel for community building and developing awareness on project outcomes and eventually enabling exploitation. The direct interactive dissemination channel will also include participation of project partners in various working groups to promote discussion and obtain feedback about AERAS outcomes.

**(ii) Organisation of industry and scientific events:** AERAS will seek to organise at least two workshops to promote an interactive dissemination of project outcomes. Such events will be important not only to disseminate project outcomes but also to obtain the opinion of experts on the current achievements and discuss ways of improving and/or enhancing the AERAS solution. To this end, in these events, we will invite various stakeholders with the knowledge and interests in the business, technical and scientific areas related to the outcomes of AERAS. Research-focused workshops will be organised in conjunction with top tier international conferences in the core research areas of the project (e.g., cyber range systems, cyber security) so as to achieve a higher visibility of project outcomes. We will also seek to have presence in industry-focused workshops and major industry events (e.g., INFOSEC).

**(iii) Scientific publications:** AERAS will aim to disseminate its outcomes through prestigious scientific publications in conferences and scientific journals. This will have several aims: (1) to increase the awareness of the scientific and research communities to project results; (2) obtain scientific feedback through peer reviewing; and (3) demonstrate the scientific soundness and credibility of project outcomes. The fora targeted for scientific publications should be top quality ones. This will serve not only the aims (1)-(3) in the best possible way but will also enhance the chance of having significant scientific recognition and impact. An equally important objective will be to ensure open access to published project outcomes as widely as possible.

Our dissemination strategy at the outset is to use of the following typical content and the main dissemination channels for the different types of targeted stakeholders:

**Healthcare CTOs:** *(i) Aim & Typical Content:* Provided information should help healthcare CTOs and healthcare IT support staff in general better understand how to apply the AERAS's approach and platform to their systems and assess the potential business benefits of it (e.g., reduced level of security risks, higher staff awareness of and preparation for cyber risks, reduced liability against cyber incidents). *(ii) Main Means:* industrial events organised by AERAS and networking events, web site, social media, mailing lists, press releases, publications in conferences and journals, and publications in business and normal press.

**Cyber system providers:** *(i) Aim & Typical Content:* Provided information should help cyber system providers understand how to apply the AERAS approach on security and security training and its platform and assess the potential business benefits of it (e.g., reduced risk and liability, increased trustworthiness, reduced complexity and improved user friendliness of their systems, etc.). *(ii) Main Means:* industrial events organised by AERAS and networking events, web site, social media, mailing lists, press releases, publications in conferences and journals, and

publications in business and normal press.

**Educators/trainers:** *(i) Aim & Typical Content:* Provided information should help communities understand how to apply the AERAS approach on security and security training and its platform and assess the technical and business implications of it. *(ii) Main Means:* scientific events organised by AERAS and networking events, web site, social media, mailing lists, press releases, publications in conferences and journals, AERAS presence in conferences and working groups.

**Scientific/research communities:** *(i) Aim & Typical Content:* Provided information should help the communities understand how to apply the AERAS approach and its platform and assess the technical and business implications of it. *(ii) Main Means:* scientific events organised by AERAS and networking events, web site, social media, mailing lists, press releases, publications in conferences and journals, AERAS presence in conferences and working groups.

### 3.3.2. Enabling use and uptake of results when available

In addition to the dissemination measures presented above, **the project will provide Open Access to all of its results.** In more detail, all project's technical deliverables and respective scientific publications will be granted open access per publisher and law regulations as set out in the Grant Agreement. Depending on the nature of the publication, the articles will be made available immediately through open access publishing ('gold' open access) (e.g. by an open access journal) or within a period of 6 months through self-archiving ('green' open access). Some AERAS partners have already established various Open Access policies (publications.city.ac.uk) supporting authors in retaining their rights to provide access to published articles, providing official repositories and making the bibliographic metadata that identify the deposited publication available to OpenAIRE (openaire.eu). Other means include finding suitable repositories via OpenAIRE, the Registry of Open Access Repositories [67] and the Directory of Open Access Repositories [68]. Thus, the Consortium will fully address the European Commission requirements and will enable the use and uptake of results when available through the support of open access.

### 3.3.3. Expected impact of the proposed measures

The following table provides a quantification of the project's dissemination activities, and sets a basis for verifying whether the project dissemination objectives have been met via key performance indicators (KPIs).

| Tool | Description | KPIs |
|---|---|---|
| Project website; technical section | Access to *AERAS* deliverables, technical results and presentations | ≥ 3.000 accesses<br>≥100 downloads |
| Professional Social Media | Regular push announcements on professional social media (LinkedIn, ResearchGate) | ≥50 announcements |
| Regular Newsletter | Bi-annual newsletter with the technical activities of *AERAS* | ≥8 newsletters |
| Brochure | High–quality electronic brochure with the technical approach and activities of *AERAS* | ≥2.000 hard copies distribution in ≥ 10 events |
| Journal and Magazine Publications | International refereed technical journals and magazines in cyber security related subjects; e.g., ACM Transactions on Information and Systems Security, IEEE Transactions on Secure and Dependable Computing, Computers and Security, IEEE Security & Privacy Magazine | ≥5 publications;<br>≥50 citations |
| Conference & Workshop Publications | International refereed technical journals and magazines in cyber security related subjects**:** ACM Conference on Computer and Communications Security, ACM Conference on Computer and Communications Security; ACM Conference on Data and Application Security and Privacy. | ≥10<br>≥100 citations |
| Special Issues in Scientific Journals | The partners will take the initiative of jointly creating at least one special issue in a scientific journal, and invite top international colleagues to be part of the initiatives. This creates a strong and long-standing link between the partners and their scientific community | ≥1<br>>50 citations |
| Workshop Organisation | *AERAS* will organise two scientific workshops, to promote an interactive dissemination of project outcomes to the relevant stakeholders. These workshops will be important not only to disseminate project outcomes but also to obtain the opinion of experts on the current achievements and discuss ways of improving and/or enhancing the *AERAS* framework. | ≥2 workshops<br>≥30 attendees (each) |
| Conference & Exhibition demos | Demos in major Cyber Security related conferences or major fairs and exhibitions (Cyber Security Europe at IP EXPO Europe, INFOSEC). | ≥2 demos |

### 3.3.4. Intellectual property rights and exploitation of results

The management of IPR will be established in the Consortium Agreement (CA), respecting the principle that IPR is and remains with the generator of it. Individual partners will be free to pursue patent filing opportunities. Any proposed disclosure of confidential project results by a Partner must first be notified to the Project General Assembly (GA) and then to project participants with a possible stake in the IPR involved. Any objections to disclosure of confidential project results (e.g., pending patent filing) will be notified to the GA. GA approval will be required for any disclosure of confidential project results outside the consortium. The GA with the support of the Project Coordinator will continuously verify these guidelines and processes and provide recommendations for improvements or solution of problems. Based on IPR ownership, access rights and use of results shall be determined and regulated according to the CA. The CA will follow the Horizon 2020 DECA template by Digital Europe and get signed by all partners in the consortium before the project starts.

### 3.3.5. Individual exploitation plans

The individual partners of *AERAS* have the following exploitation plans:

**UMIL** is a major research university and a respected player both in teaching and in research on cloud- and non-functional-related issues (including compliance, safety, SLA, security). The Department of Computer Science, to which SESAR Lab belongs, hosts the first Italian BA and MA in computer security, as well as a number of research initiatives in the same area. *AERAS* will be exploited by UMIL/SESAR Lab to: (a) further establish itself as a major player in security and trustworthiness of ICT and cloud infrastructures in the health sector, starting new educational endeavours at postgraduate level on risk analysis, cloud security and certification. In particular *AERAS* risk analysis mo dels will be at the basis of the next editions of the University's new Master on Cyber-Security Management and Governance (www.unimi.it/studenti/master/121435.htm). In addition, SESAR is a major technology transfer centre operating with a number of EU industrial partners in cloud computing, SLAs, and service/software assurance for Big Data, embedded, telecommunication, and health-related systems. Based on these partnerships, UMIL regularly holds information days, workshop, and courses on emerging technologies and methodologies. UMIL will be in a unique position to set–up a program of basic and advanced courses to complement the handbook in presenting *AERAS* techniques and methodologies to engineers and designers working in the industry as well as in academia.

**CITY** aims to exploit the AERAS platform for developing consultancy services on cyber security and cyber security training. These will be backed up by training materials regarding the use of the AERAS platform and framework that will be developed for this purpose. Such materials will be offered as part of the MSc programme of City in Cyber Security and as continuous professional development (CPD) modules for training relevant professionals. The target customers are information security professionals and officers, risk analysts, S&P certifiers, service providers who wish to prepare their systems for AERAS-based automated risk analysis, certification and CSLAs. The plan to reach objectives are the development of materials in the last 6 months of the project, the internal evaluation of use of the reference AERAS platform, the promotion of related educational offerings at security events (e.g., INFOSEC). The expected benefits are making our MSc programme in Cyber Security more attractive to prospective students.

**CUT** is unique in bringing together all Social Computing research at CUT under one roof. Michael Sirivianos collaborates closely with the security teams of Facebook and Tuenti Inc., which are already using research results from his collaborations to suppress malicious activity in their social networks. CUT will exploit the findings from the architecture and the developed cyber range application and its effect on the trainees and their behaviour to perform further research in social computing. Furthermore, CUT is also planning to investigate the potential of exploiting AERAS through its spinoff company, called IDifier Ltd. (https://www.idifier.com). IDifier aims to tackle identity fraud on the web by offering an identity acquisition and verification platform to the public, thus enabling users to verify their real-world identity documents and prove selected identity attributes to third party verifiers.

**STS** will use the outcomes of *AERAS* for strengthening its service and product portfolio. STS plan is to augment the capabilities of its security assurance and certification platform in ways that allow it to support the delivery of cyber security training programmes (e.g., providing monitoring and dynamic testing, establishing interoperability with emulation and simulation environments etc.). From a technical perspective, the strategy of STS for achieving this exploitation route is to develop mechanisms supporting the implementation of continuous assurance by executing the assurance models and developing appropriate APIs for its platform to provide access to the monitoring/testing evidence and checks required. From a business perspective, SPHYNX's strategy will be to explore ways of making use of its platform as a training tool for security auditors and for increasing the security awareness of end-users and system administrators of cyber-systems of private and public organisations in various critical sectors which are the focus markets of the company. SPHYNX will also seek to develop consultancy services in setting up training programmes for establishing cyber security assurance assessment schemes, based on the outcomes of the project.

**AEGIS** forensics visualization toolkit provides *AERAS* with an extensible framework for digital forensics real-time and post-mortem investigations, analysis and visualizations. The industrial challenge that provided motivation to

AEGIS solution and associated innovation related to *AERAS* is positioned in the interaction of three main domains, namely Advanced Visualizations for Big Data Analytics, Network and Information Security (Cyber Security), and Forensics Investigations for critical infrastructures such as the healthcare environments. *AERAS* project will help AEGIS enhance its product and services by adding new and innovative features related to cyber range, simulation and economics and expand its customers' existing portfolio.

**PAGNI** will gain a significant value for its internal IT ecosystem through AERAS. As mentioned earlier, PAGNI is the largest hospital facility in Crete and one of the largest public hospitals in the country. Growing in-house expertise will help PAGNI produce internal defense mechanisms to cope with cyber threats, reducing the cost of security monitoring by a factor of 20%, and satisfy the changing European Legislation landscape requirements (e.g., GDPR). Also, by introducing and implementing a security and privacy policy derived from *AERAS* knowledge, PAGNI expects to properly secure its network, systems and data, thus limiting (or eliminating) its risk exposure that may result in fines and damages to its reputation from a (potential) data breach (e.g., legal fees, regulatory investigation, public relations).

**UPAT** has a lot of experience in exploiting the results of various research projects. Previous experience shows that new software tools can be clinically exploited in a 5- to 10-year timeframe after the project. Partners understand that additional clinical validation with key players will be required and possibly interaction with a big software company. Clearly, IP developed in AERAS may require further steps after the project to ensure full exploitation, and appropriate partners will seek contacts to exploit to the maximum any opportunities which may come up during AERAS.

## 3.4. Quality of the proposed measures to communicate the project activities to different target audiences

*AERAS* will ensure that the research activities and their results are made known to society at large in a way that is understood by non-experts, thereby helping public understanding of science. The following groups will be targeted:

**General public:** *Aim & Typical Content:* The provided information should help the general public to understand the main concepts and approach of *AERAS* and the implications that it has for the sustainability of these systems and the value they bring to the economy, without delving into the technical details of the approach. *Main Means:* information days and Marie Skłodowska-Curie open research days and researcher nights, web site (featuring general public-oriented, non-technical overview of the project and its concept), social media, press releases, publications in normal press, public presentations, and networking events.

**Vulnerable and critical cyber-systems end user groups:** *Aim & Typical Content:* The provided information should help cyber-system end user groups to understand the main concepts and approach of *AERAS* and the implications that it has for the sustainability of these systems and the value they bring to the economy, without delving into the full technical details of the approach. *Main Means:* web site (featuring end user-oriented, non-technical overview of the project and its concept), social media, mailing lists, press releases, and publications in business and normal press, public lectures, and networking events.

**Business/policy makers:** *Aim & Typical Content:* The provided information should help policy makers to understand the main concepts and approach of *AERAS* and the implications that it has for the sustainability of these systems and the value they bring to the economy, without delving into the technical details of the approach. Emphasis should be placed on cost and benefit factors and implications at business/policy level. *Main Means:* web site (featuring business/policy-oriented, non-technical overview of the project and its concept), press releases, publications in business and normal press, public lectures, and networking events.

**EU, National, Regional and Local authorities (NRLAs):** *Aim & Typical Content:* The provided information should help NRLAs to understand how critical and/or vulnerable cyber-systems can take advantage of the *AERAS* framework. *Main Means*: Policy events, web site, social media, mailing lists, press releases, publications in conferences and journals, and publications in business and normal press.

The expected impact of the proposed measures is listed below:

| Planned Means | Success Indicators | Coverage |
|---|---|---|
| Project Website; non-technical section | >≥3.000 accesses, ≥100 downloads | Worldwide |
| Press echoes | >1 | Europe |
| Newspapers | >1 | Europe |
| Social Media | >300 followers | Worldwide |
| Public lectures and/or networking event for the general public | ≥2, >50 attendees (each) | Europe |
| Public lecture and/or networking event for policy makers | ≥2, >20 attendees (each) | Europe |
| Marie Skłodowska-Curie open research days or researchers' nights | ≥2, 100 attendees (each) | Europe |

# 4. Implementation

## 4.1. Coherence and effectiveness of the work plan, including appropriateness of the allocation of tasks and resources

The work plan of AERAS is aligned with the concept and objectives of the project and is organised in six interlinked workpackages. The project's time plan defines a four-staged cycle, with two release phases to deliver efficient, timely and relevant results to target stakeholders, and to minimise the risk from finally providing obsolete tools. Each phase is represented by a distinct set of deliverables and milestones, allowing the continuous monitoring of the project progress and safeguarding its successful completion. In more detail, the AERAS work methodology will include the:

(1) **The Baseline Phase (M1-M12)** involving elements such as the project set-up (WP1), the analysis and definition of pilot, cyber range and technology requirements, and ending with the initial reference architecture (WP2).

(2) **The Innovation Phase (M12-M34)** which focuses on technology innovation aspects and will deliver the first version of key components, such as the CRSA models and the hybrid risk assessment models (WP3), as well the Cyber Range tools (WP4), and will end with the release of the initial prototype of the platform, integrating all first version components (WP5). Considering the latter, the project's development will follow the Lean start-up methodology (theleanstartup.com) for AERAS platform delivery. To this end, two versions will be released, starting from a Minimum Viable Product (MVP), planned in M34 which will be leveraged not only to act as a proof of concept demonstrator, but to also validate the project's approach directly with key AERAS stakeholders (WP6), to test the initial hypotheses (or leap-of-faith assumptions) and adjust them prior to the pilots and the final release.

(3) **The Experimentation Phase (M34-M44)** will be driven by the MVP release at M34 and will include the evaluation of the MVP directly at the end users' (i.e. pilot) sites (WP5, M36), driving the further development and final implementation release of all key AERAS models (WP3) and components (WP4), culminating in the release of the final prototype of the integrated platform (WP5) at M44.

(4) **The Consolidation Phase (M44-M48)** in which the final integrated version of the *AERAS* solution will be deployed for the 2nd phase of the Pilot Validation (WP5) on M46. Fixes will be applied to the tools and components comprising the platform, ensuring the impact and exploitability of the project results of the cross-pilot validation (released at M48) of *AERAS* platform, also assessing its applicability in other critical domains beyond healthcare.

## 4.2. Appropriateness of the management structures and procedures, including quality management and risk management

### 4.2.1. AERAS organisation and management structure

The organizational structure of *AERAS* will involve the following bodies:

The **Project Coordinator** (PCO): The PCO will be responsible for: coordinating the project execution; receiving, managing, and distributing funding; organizing and leading project meetings; overseeing progress and producing activity reports; representing the project and reporting to the Commission. The PCO will be Prof. Ernesto Damiani of UMIL (1/ER).

The **Scientific and Technical Coordinator** (STCO): The STCO will have responsibility overseeing the execution of the project, identify risks and notify the STC, chair the STC and make suggestions to the STC and the GA regarding any technical and scientific issues requiring a decision at their level. The STCO will be Dr. Christos Kloukinas from CITY (5/ER) who has significant experience in acting as PI and technical coordinator of several H2020/FP7 projects.

The **General Assembly** (GA): The GA will consist of a designated representative from each project beneficiary authorised to commit the beneficiary to decisions related to the execution of the project within the remit of the consortium agreement. GA will be the ultimate decision-making body of the project and will be convened at least twice per year. GA will be chaired by the PCO.

The **Scientific and Technical Committee** (STC): STC will consist of WP leaders and the Scientific and Technical Coordinator (STC) of the project, who will chair it. STC will oversee the execution of the project, monitor and mitigate the technical risks arising in it and provide the overall technical and scientific direction to the consortium, ensuring that the work in WPs aligns with the project objectives. The STC report and be accountable to the GA.

**Intellectual Property Rights Committee (IPR):** The PCC may establish an IPRC if necessary to deal with intellectual property that either is introduced to the project by a partner or produced as a work package outcome. IPRC will be responsible for the definition of access rights and licensing (if required so) of the project results.

**WP Leaders** (WPLs): WPLs will be the PIs of the partners leading WPs and will have responsibility for coordinating the

WP knowledge sharing activities, overseeing the secondments and ensuring that they happen according to plan, assigning tasks to beneficiaries and individuals in line with the project's work plan. WPLs will be supported by WP co-Leaders, who will be appointed at the start of the project from another partner contributing to the individual WP. WP co-Leaders will assume WPLs responsibilities if, for any reason, WPLs are unable temporarily to carry them out.

**Advisory Board** (AB) – The project will convene an advisory board of 5 external experts from industry and academia to advice on the overall direction and relevance of project outcomes. The AB will have annual virtual or physical meetings and will report its feedback to the PCO following presentations of project outcomes. The AB will be appointed at a special GA meeting at the start of the project, following partner recommendations.

Moreover, the following management processes are defined:

**Meetings:** The GA will have at least two on-line and one physical meeting per year. It will also have as many other online meetings as required for the purposes of the project (a GA meeting may be called by the PCO or by request of at least 50% of the partners). The STC will have monthly online meetings and one physical meeting per year.

**Communication measures:** (1) A website will be set up by the coordinator and be maintained throughout the project, to present the achievements, publications, and events. (2) A project wide and five WP specific email lists will also be set up by the coordinator to enable continuous communication about the project. (3) An online document repository will also be set up for sharing reports, data and software.

**Financial management:** All partners will receive an initial advance of the EU payment aligned with their assigned work and the budget for the first year. During the following quarters, the PCO will control the appropriateness of payment according to reported work and cost claims following the H2020 funding rules and procedures.

**Monitoring mechanisms:** Qualitative and quantitative indicators will be established to evaluate research and knowledge sharing activities. These will be established in full detail by the quality plan but are expected to: (a) monitor research activities based on the number of individual and joint publications, the number of patents produced, and the development of new collaborations; and (b) knowledge sharing activities based on the number and timeliness of secondments, the number of researchers involved in them, the number of organised networking events, the level of satisfaction of the seconded researchers, and the number of dissemination and communication activities. Indicators to qualitatively assess the research activities will be the constant analysis of the general progress of the activities.

**Decision-Making, Voting & Conflict Resolution:** The Decision-Making and Conflict Resolution Process will be based on consent and transparency. All decision-making bodies (notably GA and STC) will commit to apply this. The objective is to reach agreement first by informal contact, followed by official confirmation via e-mail, letter or agreed written minutes. Decision will be taken at the level concerned, e.g. WP level if decisions affect only the WP, or escalated up to the General Assembly if they cause fundamental changes in the work plan, consortium, etc. Any party, which is a member of a consortium body, should be represented at any meeting of this body, possibly through a substitute or a proxy. No consortium body shall deliberate and decide validly unless two-thirds (2/3) of its members are present or represented (quorum). If the quorum is not reached, the chairperson of the consortium body shall convene another ordinary meeting within 15 calendar days. If quorum is not reached once more, the chairperson shall convene an extraordinary meeting, which shall be entitled to decide even if less than the quorum of Members are present or represented. Each member of a consortium body present or represented in the meeting shall have one vote. Defaulting parties may not vote. Decisions shall be taken by a majority of two-thirds (2/3) of the votes cast.

## 4.3. Appropriateness of the institutional environment (hosting arrangements, infrastructure)

All project partners have research facilities adequate for conducting research projects and knowledge dissemination/sharing activities as the ones planned in AERAS. These include office space, meeting rooms, communication equipment, and computational and network infrastructures and software platforms and tools. Moreover, the healthcare partners (PAGNI, UPAT) are committed to provide their facilities for the piloting phase, as well as dedicate their personnel in testing the effectiveness of AERAS (see KPI-15). With regards to the technical aspects of AERAS all partners are committed to provide access to the modelling, development and testing ICT tools. To this direction UMIL will make available to the project their cloud infrastructures, and CUT and CITY will provide their experimental network infrastructures respectively for software development and experimentation. Each seconded researcher will be provided with a dedicated work space and access to the above facilities, as necessary for completing successfully the secondment. They will also have access to dedicated personnel of the hosting partner, including technical and administration personnel. To support the knowledge sharing activities, all partners will provide dedicated rooms for one-on-one meetings, seminars, group work and related communication and video/audio sharing and teleconference equipment. The platforms to be used for this purpose will be established in WP1 at the start of the project and will be available to all partners. Also all partners will provide administrative support for travel arrangements, identifying suitable accommodation and getting familiarity with local customs and life, although the later will also be offered through the local hosting group of researchers.

### 4.4. Competences, experience and complementarity of the participating organisations and their commitment to the project

The complementarity of knowledge and expertise of the individual partners and the way in which it relates to carrying out the WP tasks and achieving the objectives of the project has been discussed in Sect. 2.3.1 (see Table B2.3.1). In Table B2.3.2 of the same section, we have also described how partners will be involved in the generation of new knowledge in the project and their complementary roles as knowledge producers and consumers in this respect, thus completing the picture of the synergies that will arise in the project. In general, the main exploitation of these synergies will be through the knowledge sharing and the collaborative contributions that the partners will make towards the achievement of the AERAS objectives.

## 5. References


[1] publications.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en
[2] ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_on_economic_affairs
[3] ec.europa.eu/eurostat/statistics-explained/images/d/dd/Total_general_government_expenditure_by_function%2C_2016_%28%25_of_GDP%2C_%25_of_total_expenditure%2C_million_national_currency%29.png
[4] cdn2.hubspot.net/hubfs/533449/Images/SecurityScorecard%202017%20Govt%20Cybersecurity%20Report.pdf
[5] nttsecurity.com/en-us/capabilities/threat-intelligence/global-threat-intelligence-platform
[6] hipaajournal.com/largest-healthcare-data-breaches-2017
[7] Bonaci, J. H., et al. “To Make a Robot Secure” CoRR, vol. abs/1504.04339, 2015.
[8] J. Radcliffe, “Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System,” in BlackHat USA, 2011.
[9] S. Erven et al. “Medical Devices: Pwnage and Honeypot,” in Derbycon Security Conference, Louisville, Kentucky, USA, 2015.
[10] S. Erven et al, “Medical Device Security: An Infectious Disease,” in Thotcon 2015, Chicago, IL, USA, 2015.
[11] hipaajournal.com/lack-of-security-awareness-training-healthcare-cyberattacks
[12] healthcare-informatics.com/news-item/cybersecurity/report-healthcare-employees-are-low-hanging-fruit-social-engineering-attacks
[13] ESENTIRE, “Industry Threat Report: Healthcare”, 2018, esentire.com/assets/resources/Healthcare-Threat-Report.pdf
[14] CSI/FBI, "15th Annual CSI/FBI Computer Crime and Security Survey," 2010/2011.
[15] Janne Merete Hagen, E. A. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377–397.
[16] ENISA, "The new users’ guide How to raise InfoSec Awareness" 2010, enisa.europa.eu/publications/archive/copy_of_new-users-guide
[17] Krotsiani, M.,et al. Incremental certification of cloud services. SECURWARE 2013, pp. 72-80.
[18] Dempsey K.L., et al. 2011. SP 800-137. ISCM for Federal Information Systems and Organizations.
[19] Ardagna C., et al. Big Data Assurance Evaluation: An SLA based approach, 2018 IEEE Intl Conf. on Services Comp., 2018
[20] Casola, Valentina, et al. "Automatically enforcing security SLAs in the cloud." IEEE Trans. on Services Comp. 10.5 (2017): 741-755.
[21] M. Anisetti, et al. A low-cost security certification scheme for evolving services. 19th IEEE ICWS 2012, June 2012
[22] K. Khan et al. Establishing trust in cloud computing. IT Professional, 12(5):20-27, 2010
[23] A.L. Bolgert, et al. Supporting Compliance in a Cloud Environment, 2012. google.com/patents/US20120179746
[24] M. Anisetti, et al. A Certification-Based Trust Model for Autonomic Cloud Computing Systems', ICCAC 2014
[25] M. Anisetti, et al. A Certification Framework for Cloud-based Services, ACM SAC 2016 - cloud computing 2016
[26] ENISA Threat Landscape 2015, https://www.enisa.europa.eu/publications/etl2015
[27] Internet Security Glossary, https://www.ietf.org/rfc/rfc2828.txt
[28] M. Anisetti, et al. A Test-based Security Certification Scheme for Web Services, TWEB 2013
[29] Jensen. 2011. Analysis of Attacks and Defenses in the Context of Web Services. Ph.D Thesis, Ruhr Universitat Bochum, Germany
[30] Zulkernine, et al. Towards Model-Based Automatic Testing of Attack Scenarios. ICCSRS, 2009.
[31] Jurjens. 2008. Model-based Security Testing Using UMLsec: A Case Study. Electronic Notes in Theoretical Computer Science, 220
[32] NIST. “Security and privacy controls in federal information systems and organisations,” SP 800-53-Revision 4, April 2013.
[33] National Cyber Range Overview, ieeexplore.ieee.org/abstract/document/6956748/
[34] Pham, C., et al. CyRIS: A cyber range instantiation system for facilitating security training. 7th ACM SICT, 2016.
[35] Amutio et al. MAGERIT-Methodology for Information Systems Risk Analysis and Management. Book I-The Method.

Spain, Jul 2014.
[36] Mehari 2010. Risk analysis and treatment guide. Club De La Securite De L'Information Francais, August 2010.
[37] Microsoft. The security risk management guide. 2006. microsoft.com/en-us/download/confirmation.aspx?id=6232 on 17/08/2016.
[38] Caralli A., et al. Introduction Octave Allegro: Improving the information security risks assessment process. CMU/SEI-2007-TR-012
[39] B. Karabacak et al. ISRAM: information security risk analysis method, Computers & Security, vol.24(2), pp.147—159, 2005
[40] Peng, C., et al. (2018). Modeling multivariate cybersecurity risks. Journal of Applied Statistics, 1-23.
[41] E. Damiani, et al., "A Possibilistic Risk Model for Cloud Processes," ISC Int'l J. Information Security, vol. 6, no. 2, 2014, pp. 99–123.
[42] D.S. Herrmann. Using the Common Criteria for IT security evaluation. Auerbach Publications, 2002.
[43] M. Anisetti, et al..A test-based security certification scheme for web services. ACM TWEB, 7(2):1–41, May 2013.
[44] Kourtesis, D., et al. "Increased reliability in SOA environments through registry-based conformance testing of web services." Production Planning and Control 21.2 (2010): 130-144.
[45] M. Anisetti, et al. A certification-based trust model for autonomic cloud computing systems. In Proc. of ICCAC 2014, Sep 2014.
[46] G. Koschorreck, "Automated audit of compliance and security controls,"in in Proc. of IMF 2011, May 2011, pp. 137–148.
[47] M. Anisetti, et al., ``Moon Cloud: A Cloud Platform for ICT Security Governance, IEEE Globecom2018
[48] M. Anisetti, et al., ``A knowledge-based IoT Security Checker; Euro-Par 2018
[49] Yang, Y. et al.; A survey on security and privacy issues in internet-of-things.; IEEE Internet of Things Journal 4.5 (2017): 1250-1258.
[50] Siboni, S. et al. Advanced security testbed framework for wearable IoT devices. ACM Trans. on Internet Tech. 16.4 (2016): 26.
[51] Albertson, J. et al.; Cyber security sharing and identification system; U.S. Patent No. 9,923,925. 20 Mar. 2018.
[52] Skopik, F. et al. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing; Computers Security 60 (2016): 154-176.
[53] L. Krautsevich et al.. Risk-Based Usage Control for Service Oriented Architecture, 18th Euromicro Conf PDNBP, 2010.
[54] G. Costa et al.. Metric-Aware Secure Service Orchestration. 5th ICE, EPTCS, 2012, 104, 32-46
[55] F. Massacci & A. Yautsiukhin. Modelling of quality of protection in outsourced business processes. 3rd ISIAS, 2007
[56] K. Djemame,et al., "Brokering of risk-aware service level agreements in grids," Conc. Comput.: Practice Exp., 23(7), 2011.
[57] P. Srivastava, et al., "An architecture based on proactive model for security in cloud computing," IEEE ICRTIT, 2011, pp. 661–666.
[58] C. Chen, et al., "Specify and enforce the policies of quantified risk adaptive access control," ICCSCWD'2010,, pp. 110–115.
[59] S. Pearson, "Toward accountability in the cloud," IEEE Internet Comput., vol. 15, no. 4, pp. 64–69, Jul./Aug. 2011.
[60] owasp.org/index.php/Data_Validation
[61] Grossman, J., et al. XSS attacks: cross site scripting exploits and defense. Syngress.
[62] Clarke-Salt, J. (2009). SQL injection attacks and defense. Elsevier, 2007
[63] ww2.frost.com/frost-perspectives/h-healthcare-2025
[64] nationaljournal.com/md/652678/healthcare-industry-is-expected-see-17-4-growth-employment-2024
[65] Global Digital Health Market 2018-2022, researchandmarkets.com/research/6gqstc/global_digital?w=4
[66] https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy/innovation-union_en
[67] http://roar.eprints.org/
[68] http://www.opendoar.org/
[69] nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs
[70] csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

# 6. Ethics Issues

## 6.1. Ethics

The *AERAS* Consortium is fully mindful of the ethical aspect and the social impact of the proposed research activities and it absolutely respects the ethical rules and standards of H2020, as well as those reflected in the Charter of Fundamental Rights of the European Union and the Data Protection Directive (Directive 95/46/EC). In this respect, in parallel with the development of the *AERAS* concept for the preparation of the proposal, the *AERAS* partners also lay particular emphasis on the identification of the ethical issues that are expected to arise in the context of the *AERAS* framework.

As a result, we anticipate that some operations envisioned by *AERAS* could inevitably fall within the ambit of Directive 95/46/EC, as they imply processing of data that can relate to identified or identifiable persons.

In order to guarantee the privacy of the users at the *AERAS* units and safeguard the confidentiality and protection of the data collected in the project, the following security and privacy controls will be applied:

- The *AERAS* Project Management Board (see Section 3) will continuously assess the legal, ethical and societal impact of the solutions developed within the project and the potential future implementations and deployments based on them.
- The basic approach of *AERAS* will be to reduce the collection and even initial storage of personal data to the absolute minimum.
- Any data or information about a person will be processed, communicated and stored in a manner that preserves privacy and confidentiality, regardless of how this data was acquired.
- The acquired data will under no circumstances be used for commercial purposes or shared with any third parties.
- *AERAS* will follow the formal procedures that are explicitly defined within each partner organization to protect the anonymity of data that are shared among the Consortium.

We should hasten to clarify that as described above, our approach will be to reduce the amount of personal data to the absolute minimum in the interest of privacy, and we will resort to synthetic data whenever possible. However, because the medical partners are aimed at future deployments of the AERAS platform after the project ending, where real data about their IT systems might be handled, at any points of the information flow where sensitive data is gathered, directly or indirectly affecting the privacy of end-users, strict access-control policies will be enforced. These activities can happen only after the end of the AERAS project and they are not covered by this Grant Agreement.

Furthermore, we shall implement privacy-enhancing countermeasures. These will be based on the methodology of statistical disclosure control, specifically, via anonymous micro-aggregation techniques striving to attain an optimal trade-off between data privacy and usability.

Finally, it is important to note that no real data will be used during the pilots' validation. All data included and used in the virtual environments during the training, will be automatically fabricated and will not be collected from the pilots.

## 6.2. Ethics Committee

For Personal Data protection, the Data Protection Officer (DPO) required by GDPR will be alerted for each *AERAS* Consortium partner. Also an ethics committee will be setup for the project. The ethics committee will be responsible for resolving all probable ethics issues during project execution. The composition of the Ethics committee will be detailed in deliverable D1.1: Data Quality Plan.

## 6.3. Ethics requirements

The independent ethics experts identified six pre-grant requirements and three post-grant requirements. This section describes how these requirements are being addressed by *AERAS*.

### 6.3.1 Pre-grant requirements

**Pre-grant requirement H1**

**Description:** The procedures and criteria that will be used to identify/recruit research participants must be clarified in the grant agreement before signature.

**Resolution:** Participation of Humans in *AERAS* will be only on a voluntary basis. Contact with participants will be

established initially and potential participants will be informed them about the aims of the project, the research under-taken and how any data collected from them will be used will be provided. The same details will be provided in writing. In any period of this voluntary participation, a participant may acquire additional information. In addition, participants may withdraw at any time without any consequence and any data collected from them up to the point of their withdrawal will be destroyed.

**Pre-grant requirement H2**

**Description:** Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) for recruitment of participants and processing of personal data must be specified in the grant agreement before signature.

**Resolution:** Extraordinary care will be taken to receive appropriate and legally valid informed consent from the participants. This will only be carried out with the prior, free, informed and expressed consent of the participating individuals. This will be done in accordance with all applicable international laws and ethical guidelines related to the protection of personal data as well as internationally accepted rules on ethics and human rights. Principles that *AERAS* will follow in this context are information disclosure, data anonymization, the right to withdraw, etc. A potential participant interested in being involved in *AERAS* activities, will be given a written informed consent form explaining the scope and the procedures to be followed in his participation and if participant agrees, both sides will sign this informed consent. A template of such a form is provided below.

*<< Consent form starts here>>*

## Informed consent form template

**Title of the training:**
[Insert title]

**Principal investigator:**
[Name]
[Department]
[Address]
[Phone]
[Email]

**Purpose of training**

You are being asked to take part in a training demonstration. Before you decide to participate in this training pilot, it is important that you understand why it is performed and what it will involve. Please read the following information carefully. Please ask the researcher if there is anything that is not clear or if you need more information.

The purpose of this pilot training is to *[describe]*

**Training procedure**

*[describe what is going to happen]*

**Contact information**

If you have questions at any time about this pilot training, you may contact *[add contact information]*

**Personal data**

During your participation in this training any personal data collected will be anonymized.

**Voluntary participation**

Your participation in this training is voluntary. It is up to you to decide whether or not to take part in this. If you decide to take part in this pilot, you will be asked to sign this consent form. After signing the consent form, you will still be free

to withdraw at any time and without giving a reason. If you decide to withdraw your participation before the end of the project, any data collected for you will be destroyed and you will be notified accordingly. Furthermore, at any stage during the project, you may request to obtain any data that have been collected for you and you will be entitled to get these data. Also, during the project, you may request the deletion of any of the data that have been collected for you. Upon the receipt of such a request, the project will delete the data that you requested to be deleted and provide you with evidence that the requested deletion was made. All the data collected during the project will either be deleted at the end of it or will be maintained in a fully anonymized form, which under no circumstances will allow the tracing of such data back to you, for research purposes

**Consent**

I have read and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study.

Participant's signature_____Date _____

Investigator's signature_____Date _____

*<<Consent form finishes here>>*

*<< Information Sheet starts here>>*

## Information Sheet

## I. About the research Project

**AERAS EU-funded Project**

The AERAS (A CybEr range tRaining platform for medicAl organisations and systems Security) project (hereafter, the "**Project**") aims to develop a realistic and rapidly adjustable cyber range platform (the "**Platform**") for systems and organisations in the critical healthcare sector, to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical cyber-systems and organizations against advanced, known and new cyber-attacks, and reduce their security risks.

The Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 872735. The project is funded under the EU call H2020-MSCA-RISE-2019 and lasts 4 years ([START DATE – FINISH DATE]).

**Research purposes**

The platform will be based on an evidence-based approach where virtual cyberwarfare and simulations are configured according to evidence regarding: (i) the occurrence of cyber threats, and (ii) the effectiveness of the operation of the internal and external system defence mechanisms.
Evidence will be collected by multi- faceted real-time monitoring and assessed according to Cyber Range Security Assurance (CRSA) models specifying potential cyber-attacks, the security mechanisms used against them, and the methods for assessing their effectiveness (the "**Research**").

**Project Partners**

The partners of the AERAS Project are the following (the "**Partners**"):

| | Organisation Name | Country |
|---|---|---|
| 1 | Universita Degli Studi di Milano (UMIL) | Italy |
| 2 | City University of London (CITY) | UK |
| 3 | Technologiko Panepistimio Kyprou - Cyprus University Of Technology (CUT) | Cyprus |
| 4 | SPHYNX Technology Solutions AG (STS) | Switzerland |
| 5 | AEGIS IT Research UG (AEGIS) | Germany |
| 6 | Regional University Hospital of Heraklion (PAGNI) | Greece |
| 7 | Panepistimio Patron - University Of Patras | Greece |

## II. Information Sheet (Privacy Policy)

**Scope of this policy**

This information sheet (hereafter "Privacy Policy") describes how your personal data is collected, used and otherwise processed in the context of the EU AERAS Project funded under the H2020 research programme, contract no. 872735 (hereafter the "Project"). This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- "**We**" or "**us**" refer to the Partners of the AERAS Project listed in Section I above, who will process your personal data as data controllers and as described herein. The Project Partners can be contacted collectively through the contact details provided below and notably by sending an email to [email address].
- "**Data Protection Legislation**" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

**What personal data is processed?**

In the context of the Project, your personal data is processed by the Partners, as follows:

- **Processing purpose(s)**: for the purpose of carrying out the research in the Project, as described in Section I above.
- **Processed data categories**: [first name, last name, organisation, title / function, email address, any information you decide to share with us through discussions, interviews, correspondence and questionnaires, sound and/or video recordings (where applicable)]
- **Source of data**: from you, directly through the Informed Consent Form & Information Sheet, [discussions, interviews, correspondence and questionnaires].
- **Legal basis**: Your consent, as provided in Section III. You may withdraw that consent at any time you choose and at your own initiative by contacting us at [email address]. The withdrawal of your consent will not affect the lawfulness of the collection and processing of your data based on your consent up until the moment where you withdraw your consent.

**How long is your personal data stored?**

We retain your personal data for the duration of the Research Project (i.e. until [FINISH DATE]) or for a shorter period as long as your data are required to fulfil the activities set out in the Informed Consent Form and this Privacy Policy.

**Is your personal data transferred outside the European Economic Area (EEA)?**

We do not intend to transfer the data that we collect from you to a destination outside the EEA.

**What are your rights?**

Once you have provided your personal data, several rights are recognised under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to withdraw your consent:** you may withdraw your consent at any time you choose and at your own initiative by contacting us at [email address]. The withdrawal of your consent will not affect the lawfulness of the collection and processing of your data based on your consent up until the moment where you withdraw your consent.
- **Right to access and rectify your data**: you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to [email address]. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure**: you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing**: under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.
- **Right to data portability**: under certain circumstances described in the Data Protection Legislation, you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.

To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

**What security measures are put in place?**

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data. In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

**How can we be contacted?**

Questions, comments, remarks, requests, complaints or feedback regarding this Privacy Policy are welcome and should be addressed to: [email address].

*<< Information Sheet finishes here>>*

**Pre-grant requirement POPD1:**

**Description:** A description of the technical and organizational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be specified in the grant agreement before signature.

**Resolution:** The participation at the training is voluntary. It is up to the trainee to decide whether or not to take part in this. If she/he decide to take part the consent form will be asked to sign. After signing the consent form, the trainee is still free to withdraw at any time and without giving a reason. If she/he decide to withdraw before they training is completed, any data collected by you will be returned to her/him or destroyed.

**Pre-grant requirement POPD2**

**Description:** A description of the security measures that will be implemented to prevent unauthorized access to personal data or the equipment used for processing must be specified in the grant agreement before signature.

**Resolution:** During AERAS execution we do not foresee to collect any personal data. However, in the rare case that such need will come up, any personal data that may be collected during the execution of AERAS, will be anonymized and stored to a secure storage location. The AERAS Project Technical Committee will be responsible for the personal data protection. Collected data will be stored throughout the project execution time and will be deleted after the

project ends. The data repository will be decided by the project consortium adopting appropriate physical and IT security measures (authentication, authorization and accountability).

**Pre-grant requirement POPD2**

**Description:** Detailed information on the informed consent procedures in regard to the collection, storage, and protection of personal data must be provided in the Description of Action before grant agreement signature.

**Resolution:** This requirement is covered together with pre-grant requirement H2 above.

**Pre-grant requirement POPD3**

**Description:** Description of the anonymization/pseudonymization techniques that will be implemented must be specified in the grant agreement before signature.

**Resolution**: All the data collected or used during the training will be stored in anonymized form without any link to the original sources. Anonymization will be performed via non-reversible hashing whenever appropriate.

**Pre-grant requirement POPD4**

**Description:** In case of further processing of previously collected personal data, an explicit confirmation that the beneficiary has lawful basis for the data processing and that the appropriate technical and organizational measures are in place to safeguard the rights of the data subjects must be included in the grant agreement before signature.

**Resolution:** In *AERAS* no further processing of previously collected personal data is foreseen. In the case that something like this comes up, all relevant authorization that may be required will be obtained and will be reported in the deliverable D7.3: POPD-Requirement No. 9 (month 6).

### 6.3.2 Post-grant requirements

To address Post-grant ethics requirements for *AERAS* a new work package (WP7) with 3 additional deliverables, D7.1: H-Requirement No. 3, D7.2: POPD-Requirement No. 4 and D7.3: POPD-Requirement No. 9. Has been added in AERAS's work plan (see annex A).

**Post-grant requirement H1**

**Description**: All required opinions/approvals by ethics committees and/or competent authorities for the research with humans must be obtained before starting the relevant activity, kept on file and submitted upon request.

**Resolution:** All required opinions/approvals by ethics committees and/or competent authorities related to *AERAS* activities will be provided in D7.1: H-Requirement No. 3 (month 12).

**Post-grant requirement POPD1**

**Description**: The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable.

**Resolution**: In the context of WP7: Ethics the Data Protection Officers of the host institution and other consortium members required by GDPR will be identified and alerted by each partner. The Università di Milano DPO Prof. Pierluigi Perri will coordinate their overseeing of the project. The complete list of the Consortium DPOs and data protection policies will be contained in D7.2: POPD-Requirement No. 4 (month 1).

**Post-grant requirement POPD2**

**Description**: The beneficiary must evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art. 35 General Data Protection Regulation 2016/679. The risk evaluation and the opinion must be submitted as a deliverable.

**Resolution:** This activity will be carried out by the *AERAS* ethics committee and will be reported in D7.3: POPD-Requirement No. 9 (month 6). An addition additional opinion will be requested from the permanent ethics committee of the coordinator (https://www.unimi.it/en/node/449). The Data Protection Officer of the Università degli Studi di Milano Prof. Pierluigi Perri will be informed of project activities.


**Marie Skłodowska-Curie Actions (MSCA)**
**Research and Innovation Staff Exchange (RISE)**
**H2020-MSCA-RISE-2019**

**Project Acronym: AERAS – Project Number: 872735**
**Annex 1 to the Grant Agreement**
**(Description of the Action)**
**Part B**