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

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

AERAS

A CybEr range tRaining platform for medicAl organisations and systems Security

D3.2: AERAS Models and CRSA-driven Cyber Range Programme V1 [1†]

Abstract: This deliverable presents the initial outcomes of tasks T3.2, T3.3, and T3.4, focusing on the development of AERAS Cyber Range Security Assurance (CRSA) models and their dynamic adaptation, as well as the AERAS Cyber Range Simulation and Training (CRST) programs and hybrid risk analysis models. It outlines the first version of these models and the tools supporting them and provides guidance for their ongoing development, which will be further detailed in the subsequent deliverable, D3.3.

Contractual Date of Delivery	30/09/2024
Actual Date of Delivery	31/12/2024
Deliverable Security Class	Public
Editor	Kostantinos Papadamou (TRID)
Contributors	Zois Nearchou (TRID), Kostantinos Papadamou (TRID), Dimitris Plachouris (UPAT), Panagiotis Archontidis (CUT), Theodoros Christophides (CUT), Pantelitsa Leonidou (CUT), Nikos Salamanos (CUT), Konstantinos Kalais (CUT), Katerina Christopguidou (CUT), Stelios Christophides (LIBRA), Nastasia Michael (LIBRA), Nikos Chrysostomou (LIBRA), Georgia Christophidou (LIBRA), Evangelous Floros (PAGNI), Angelos Afxentiou (EAIN), Marinos Raimondou (EAIN), Lucas Papadoulas (EAIN)
Quality Assurance	Fulvio Frati (UMIL) Pantelitsa Leonidou (CUT)

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

The *AERAS* Consortium

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

Document Revisions

Internal Reviewers

1. Fulvio Frati (UMIL)
2. Pantelitsa Leonidou (CUT)

Revisions

Version	Date	Contributors	Overview
v1.0	30/12/2024	Editor	Final corrections and final deliverable version ready to be submitted
v0.9	17/12/2024	Editor, Authors, Internal Reviewers	Deliverable internal review and final changes completed
v0.8	13/12/2024	Editor, Internal Reviewers	Internal Review of the final draft of the Deliverable
v0.7	09/12/2024	Authors	Added Section 6 - "Conclusions"
v0.6	04/12/2024	Authors	Final Section 5 - Finalized CRSA and CRST models for both Pilots
v0.5.2	30/11/2024	Authors	Added Section 5.2 "Pilot 2 - Healthcare Authority (PAGNI)"
v0.5.1	18/11/2024	Authors	Added Section 5.1 - "Pilot 1: Smart Hospital Environment (UPAT)"
v.0.5.0	04/11/2024	Authors	Added initial version of Section 5 - "AERAS CRSA-Driven Cyber Range Programmes Specification"
v0.4	21/10/2024	Authors	Added Section 4 - "AERAS CRSA-driven Training Programmes Definition"
v0.3	11/10/2024	Authors	Added Section 3 - "Pilot Requirements, Environments, and Training Programmes Specifications"
v0.2	27/09/2024	Authors	Added Section 2 - "Security Assurance Landscape and Threat Analysis"
v0.1.2	16/09/2024	Authors	Final version Table of Contents
v0.1.1	09/09/2024	Editor	First Draft of the Executive Summary and the Introduction Section
v0.1	04/09/2024	Editor	First draft of the Table of Contents (ToC)

Executive Summary

This deliverable, D3.2: AERAS Models and CRSA-driven Cyber Range Programme V1, outlines the foundational outcomes of Tasks T3.2: CRSA-driven Cyber Range Program Development and T3.4: Hybrid Cyber Security Risk Analysis Models, representing a pivotal milestone in the development of the AERAS platform. As the first iteration of these components, this report focuses on establishing the Assurance Tools Layer, a critical part of the platform architecture designed to bridge the gap between cybersecurity assurance and cyber range simulation and training.

Key deliverables of this report include the first version of the AERAS CRSA models, which extend traditional security assurance frameworks by incorporating adaptive and dynamic features. These enhancements ensure that the CRSA models can drive the development of Cyber Range Security Training (CRST) programs that are not only effective but also tightly aligned with the evolving security needs of the adopting organization. The procedures outlined in this deliverable provide the foundation for the dynamic adaptation of CRSA models, enabling organizations to maintain robust and responsive security postures in the face of ever-changing cyber threats.

In addition, this deliverable introduces the first version of the hybrid cybersecurity risk analysis models, which form the backbone of the Cyber-system Real-time Risk Evaluator (CRSE) component. The CRSE leverages an organization's "infrastructure definition" to assess its cybersecurity risks. By analyzing system vulnerabilities, risk exposure, and potential threat vectors, the CRSE provides feedback for the adaptation of CRSA models and the optimization of CRST training programs, ensuring they remain relevant and effective.

Overall, this deliverable provides a first outcome of tasks T3.2 and T3.4 detailing the models and training programmes developed thus far and sets the stage for subsequent iterations. Finally, the upcoming deliverable D3.3, will build on this foundation, refining and expanding the components and processes outlined herein.

Table of Contents

List of Figures

List of Tables

Table of Abbreviations

AES	Advanced Encryption Standard
CC	Common Criteria
CCHIT	Certification Commission for Health Information Technology
CIS	Critical Security Controls
CMMC	Cybersecurity Maturity Model Certification
COBIT	Control Objectives for Information and Related Technology
CRSA	Cyber Range Security Assurance
CRSE	Cyber-system Real-time Risk Evaluator
CRST	Cyber Range Simulation and Training
CS	Cybersecurity
CSA	Cloud Security Alliance
CT	Computed Tomography
DIS	Diagnostic Imaging Services
DMZ	Demilitarized Zone
ERP	Administrative-economic Services
EUCC	EU Cybersecurity Certification Framework
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HITECH	Health Information Technology for Economic and Clinical Health
HITRUST	Health Information Trust Alliance
HTTPS	Hypertext Transfer Protocol Secure
ICU	Intensive Care Unit
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITGR	IT Governance and Risk
ITIL	Information Technology Infrastructure Library
LTO	Long-Term Archiving Systems
LIS	Laboratory Services
MRI	Magnetic Resonance Imaging

NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PACS	Picture Archiving and Communication System
PET	Positron Emission Tomography
REST	Representational State Transfer
RIS	Radiology Information System
SMTP	Simple Mail Transfer Protocol
SOC	Service Organization Control
SPECT	Single-photon Emission Computerized Tomography
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VM	Virtual Machine
WP	Work Package
X-RAY	X-Radiation
YAML	Yet Another Markup Language
ZTA	Zero Trust Architecture

1 Introduction

This deliverable, **D3.2: "AERAS Models and CRSA-driven Cyber Range Programme V1"**, documents the primary outputs of Tasks **T3.2: "CRSA-driven Cyber Range Program Development"** and **T3.4: "Hybrid Cyber Security Risk Analysis Models"** and serves as a major outcome of the work conducted within WP3. Specifically, it details the initial development of the CRSA models and the key components of the **Assurance Tools** and **Cyber Range Tools** layers of the AERAS platform. Together, these components enable the realization and dynamic adaptation of the **Cyber Range Security Assurance (CRSA)** models and the associated **Cyber Range Simulation and Training (CRST)** programs.

The deliverable focuses on the development of reference CRSA models and CRST programs tailored for the two pilot activities of the AERAS project. These CRSA models are specified based on the language and framework developed in **Task T3.1: "CRSA Language Definition and Tool Support"**. The design and implementation of the models and resulting CRST programs incorporate a comprehensive analysis of existing security assurance profiles (e.g., Common Criteria protection profiles and CPA commercial product assurance security schemes) for the targeted pilot organizations' systems, known threats to underlying components, and the deployed security controls.

Additionally, the CRSA models and their corresponding CRST programs were developed based on 1) the evaluation of existing assurance schemes; 2) the identification of threats within the piloting environments; and 3) the specific needs of each organization participating in each pilot, as derived from responses to questionnaires completed by the pilot participants involved in the two pilots. Further details about the questionnaire process, participants, results, and conclusions can be found in the related deliverable D5.3: AERAS Initial Prototype Pilot Validation Report, which has been drafted in parallel with this deliverable due to their interconnected objectives.

To date, six (6) unique training scenarios have been modeled for the two pilots: three for the University of Patras (UPAT) Smart Hospital Environment pilot and three for the PAGNI Healthcare Authority pilot, with some scenarios shared between the pilots due to overlapping security needs. The development process for the CRSA models and CRST programs follows a structured approach comprising the following phases:

1. **Analysis of the pilot organization's environment:** Comprehensive evaluation to identify potential threats, vulnerabilities, and organizational needs.
2. **Creation of core CRSA Models and sub-models:** Development of the Cyber System model, which describes the infrastructure of the organization. At this stage, additional sub-models are created, including a) the Cybersecurity Assurance model; 2) the Risk Assessment model; and the 3) Threats and Incidents model. Together, these sub-models form the complete CRSA model.
3. **Definition of CRST Programs:** Using the CRSA models, which include detailed information on the organization's infrastructure and cybersecurity threats, the full CRST training programs are defined. These training programs leverage simulation capabilities provided by the Cyber Range Tools layer to evaluate trainee performance automatically.

The CRSA models and CRST programs developed for the two pilots and documented in this deliverable are designed to be generic and abstract, enabling their adaptation to any type of infrastructure or environment. Their agnostic nature ensures compatibility with diverse systems and programming languages, allowing them to be translated and applied across different organizational contexts.

1.1 Role of the Deliverable

The primary role of this deliverable, D3.2: AERAS Models and CRSA-driven Cyber Range Programme V1, is to document the first versions of the AERAS CRSA models and the associated Cyber Range Simulation and Training (CRST) programs developed for the pilot projects of the AERAS initiative. This deliverable consolidates the outcomes of Task 3.2: CRSA-driven Cyber Range Program Development and Task 3.4: Hybrid Cyber Security Risk Analysis Models, focusing on the creation of tailored CRSA and CRST models for the pilot organizations. By presenting these initial models, this deliverable provides tangible examples of how the CRSA models are defined and how they support the development of adaptive CRST programs. These efforts form the foundation for validating the effectiveness of the AERAS platform within the context of the two pilots and set the stage for further refinement in subsequent deliverables.

1.2 Relationship to other Deliverables

This deliverable, **D3.2: "AERAS Models and CRSA-driven Cyber Range Programme V1"**, is closely linked to and builds upon **D3.1: "CRSA Models and CRSA-driven Cyber Range Programme Specification Language"**, which defines the language used to create the CRSA and CRST models and training programs for the AERAS pilots. The specification language outlined in D3.1 serves as the foundational framework for developing the models and programs documented in this deliverable.

Additionally, this deliverable D3.2 is heavily dependent on **D5.3: "AERAS Initial Prototype Pilot Validation Report"** (WP5), which provided the requirements and key cybersecurity needs and risks for each organization participating in the pilots. The alignment with D5.3 ensures that the CRSA and CRST models are tailored to the specific operational contexts of the pilot organizations, enabling targeted and effective training programs. Finally, this deliverable will provide input for the final deliverable of WP3 (D3.3 "AERAS Models and CRSA-driven Cyber Range Programme V2") as it lays the foundation for the definition and development of the AERAS models and CRSA-driven Cyber Range Programme.

1.3 Structure of the document

The rest of the deliverable is structured as follows. **Section 2** provides an overview of existing security assurance profiles and schemes, along with the security landscape of the two pilot environments. **Section 3** outlines the requirements and the environment architecture of each organization participating in the pilots of AERAS, detailing their objectives and scope. Next, **Section 4**, outlines the training program definitions for the two pilot activities of AERAS describing the defined training scenarios for each pilot. In **Section 5** we present the defined and developed CRSA models and CRST training programs for the two pilots, including all relevant details, examples, and the developed procedures that support the dynamic adaptation of the CRSA models. Finally, **Section 6** concludes the deliverable with final remarks and outlines the next steps in WP3.

2 Security Assurance Landscape and Threat Analysis

The development of the reference CRSA models and CRST training programs for the two pilot activities of the AERAS project is deeply rooted in a detailed analysis of the current security landscape. This includes the evaluation of existing security assurance schemes, the identification of known threats targeting the various components within the pilot organizations' infrastructures, and the assessment of the security controls implemented in their systems. This section explores these foundational elements in detail, establishing the necessary context for tailoring the CRSA models and CRST training programs to the unique requirements of the pilot environments. By understanding these critical factors, the AERAS project ensures that the developed models and programs effectively address the cybersecurity challenges faced by the pilot organizations.

2.1 Security Assurance Schemes Overview

This subsection presents an analysis of the existing security assurance landscape, focusing on widely adopted security schemes and standards relevant to the two pilot activities of the AERAS project. These assurance schemes provide foundational principles, best practices, and evaluation methods for ensuring the security and resilience of organizational systems.

2.1.1 General Security Assurance Schemes

Table *1* below provides an overview of the widely applicable and well-known security assurance schemes considered and analyzed in the context of the two AERAS pilots. These schemes serve as a reference for the design and implementation of the CRSA models and CRST training programs.

#	Security Assurance Scheme	Description
1	**ISO/IEC 27001** [1]	ISO/IEC 27001, formally known as ISO/IEC 27001:2022, is an international security standard that outlines the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). It helps organizations secure their information assets and manage data breaches effectively. The standard is applicable across various industries, particularly in sectors that handle sensitive data such as healthcare and IT. Key features include risk management processes, compliance with legal requirements, and a structured approach to managing information security risks.
2	**ISO/IEC 27002** [2]	ISO/IEC 27002:2022 is a standard that provides best practice recommendations for information security management. ISO/IEC 27002 offers a detailed set of controls and guidelines to manage and protect information assets. It is designed to help organizations select, implement, and manage security controls that align with their specific needs and risk management processes.
3	**ISO/IEC 27018** [3]	ISO/IEC 27018:2019 is a privacy standard specifically addressing the protection of personal data in the cloud. It provides guidelines for cloud service providers to ensure that personal data is handled according to privacy principles and regulations.

4	**ISO/IEC 27032** [4]	ISO/IEC 27032:2023 is a guideline for improving cybersecurity, with a focus on collaboration and coordination between stakeholders, including governments, private organizations, and end users. It provides a framework for managing cyber risks and protecting digital assets.
5	**NIST Cybersecurity Framework (CSF) 2.0** [5]	The NIST Cybersecurity Framework (CSF) is a voluntary set of standards, guidelines, and practices to help organizations manage cybersecurity risk. It is designed for both critical infrastructure and non-critical sectors, covering five core functions: Identify, Protect, Detect, Respond, and Recover. It is widely adopted across various industries and is recognized for its flexibility and adaptability, making it suitable for organizations of all sizes.
6	**NIST SP 800-53 (Rev.4)** [6]	NIST SP 800-53 (Rev.4) is a security compliance standard that provides a catalog of security and privacy controls for federal information systems. It is part of the NIST Risk Management Framework and is used to help organizations implement effective cybersecurity measures for federal and critical infrastructure systems. The standard includes controls across various families, such as access control, incident response, and system protection, aimed at safeguarding sensitive data against a range of threats. It is applicable not only to federal agencies but can also be adopted by any organization handling sensitive information.
7	**NIST SP 800-37 (Rev.2) - Risk Management Framework (RMF)** [7]	The RMF (NIST SP 800-37 - Rev.2) is a structured approach for identifying, assessing, and managing risks related to information systems. It is used primarily by federal agencies to ensure that their information systems meet security and privacy requirements throughout their lifecycle.
8	**GDPR (General Data Protection Regulation)** [8]	The GDPR is a regulation in the European Union that focuses on data protection and privacy. It applies to any organization processing personal data of EU residents and mandates transparency, data subject rights, and data breach reporting.
9	**CIS Controls**	The CIS Controls are a set of best practices for securing IT systems and data. They provide a prioritized, prescriptive approach to cybersecurity, focusing on critical controls like inventory and control of hardware and software assets, and continuous vulnerability management. CIS focuses more on the technical part of the security practices compared to ISO/IEC 27001.
10	**COBIT 5** [9]	COBIT 5 is a governance framework for the management and control of enterprise IT developed by ISACA. It covers risk management, compliance, and IT governance, aiming to ensure that organizations achieve their objectives and manage IT-related risks effectively, thus ensuring compliance with regulations. COBIT is widely used across industries to optimize IT investments and improve overall business performance. Its key features include a focus on

		stakeholder needs, end-to-end coverage of enterprise processes, and a structured approach to IT governance.
11	**CSA CCM (Cloud Security Alliance Cloud Controls Matrix)**	The CSA CCM is a cybersecurity control framework designed to help organizations assess the security posture of cloud providers. It includes control objectives in areas such as governance, risk management, compliance, and security operations.
12	**CMMC (Cybersecurity Maturity Model Certification)**	CMMC is a framework established by the U.S. Department of Defense (DoD) to assess the maturity of cybersecurity practices in defense contractors. It includes five levels of maturity, ranging from basic practices to advanced, and is aimed at protecting controlled unclassified information (CUI) in the supply chain of defense contractors.
13	**Zero Trust Architecture (ZTA)** [10]	Zero Trust Architecture (ZTA) is a security framework that assumes no implicit trust, regardless of whether a user or device is inside or outside the network perimeter. It enforces strict access control and authentication measures, validating every request to access resources.
14	**OWASP Top Ten** [11]	The OWASP Top Ten is a widely recognized list of the most critical web application security risks. It is updated regularly by the Open Web Application Security Project (OWASP) and includes vulnerabilities such as injection flaws, broken authentication, sensitive data exposure, and security misconfigurations.

Table 1. Generally Applicable Security Assurance Schemes

2.1.2 Healthcare-specific Security Assurance Schemes

In this subsection, we examine healthcare-specific security assurance schemes, focusing on the standards and frameworks tailored to address the unique security and compliance requirements of the healthcare sector. Given the sensitivity of healthcare data and the critical nature of healthcare infrastructure, these schemes play a vital role in safeguarding systems, ensuring data privacy, and managing risks. **Table *2*** below provides an overview of the most relevant sector-specific security standards and frameworks considered within the context of the two AERAS pilot activities.

#	**Security Assurance Scheme**	**Description**
1	**ISO/IEC 27799** [12]	ISO/IEC 27799:2016 is an international standard that provides guidelines for information security management in healthcare organizations. It focuses on protecting personal health information (PHI) and ensuring privacy in compliance with regulations like HIPAA.
2	**HITRUST CSF (Health Information Trust Alliance Cybersecurity Framework)** [13]	HITRUST CSF is a certifiable framework designed to help organizations in the healthcare sector meet the requirements of various regulations and standards, including HIPAA, HITECH, and ISO/IEC 27001 [1]. It provides a comprehensive and scalable approach to managing healthcare cybersecurity risks, with a focus on information security, privacy, and risk management.

3	**HIPAA (Health Insurance Portability and Accountability Act)** [14]	HIPAA is a U.S. law that establishes national standards for the protection of health information. It sets requirements for safeguarding electronic health records (EHRs) and ensures that healthcare organizations maintain patient data privacy and security.
4	**HITECH Act (Health Information Technology for Economic and Clinical Health Act)** [15]	The HITECH Act supports the adoption of health information technology, including secure exchange of electronic health records (EHRs). It encourages the use of encryption and other safeguards to protect patient data, ensuring compliance with HIPAA requirements.
5	**NIST SP 800-53 for Healthcare** [16]	NIST SP 800-53 is a catalog of security and privacy controls for federal information systems. Its application to healthcare focuses on protecting electronic health information systems, ensuring the integrity and confidentiality of patient data.
6	**NIST Cybersecurity Framework for Healthcare** [16]	This adaptation of the NIST Cybersecurity Framework is tailored for healthcare organizations. It helps them manage cybersecurity risks related to health information systems, ensuring the confidentiality, integrity, and availability of patient data.
7	**CCHIT (Certification Commission for Health Information Technology)**	CCHIT is an organization that provides certification for health IT products, including Electronic Health Records (EHR) systems, ensuring that they meet federal security and privacy requirements for patient data protection.

Table 2. Healthcare-specific Security Assurance Schemes

2.2 Security Assurance Profiles, Compliance Standards, and Product Guidelines

In this subsection, we present the current security assurance profiles, compliance standards, and product guidelines that have been identified as relevant and applicable to the AERAS project and its pilot activities. These profiles and standards play a critical role in shaping the design and implementation of the CRSA models and CRST training programs by providing structured requirements, evaluation criteria, and best practices. They are considered for ensuring alignment with established security practices, regulatory compliance, and product security guidelines, ultimately supporting the overall objectives of the AERAS platform. The identified profiles, standards, and guidelines are summarized in **Table *3*** below.

#	Assurance Standard / Profile	Description
1	**Common Criteria (ISO/IEC 15408)** [17]	ISO/IEC 15408:2022, also known as Common Criteria, is an international standard for evaluating the security properties of IT products and systems. It includes components like Protection Profiles, which define security requirements for specific product categories, and a structured evaluation process to assess compliance with these requirements. This framework is widely used in certifying products for government, defense, and regulatory bodies, providing assurance on the security features of a product.
2	**EUCC (EU Cybersecurity Certification Framework)** [18]	The EU Cybersecurity Certification Framework is a comprehensive set of rules and criteria to ensure top-level

		cybersecurity for Information and Communication Technology (ICT) products, services, and systems in the European Union. Developed by ENISA [19] under the EU Cybersecurity Act, it aims to standardize cybersecurity measures across the EU, providing a unified approach to certification. This framework enhances trust and security in digital products and services, addressing fragmentation in existing national certification schemes.
3	**SOC 2 Type 2 (Service Organization Control Type 2)** [20]	SOC 2 (System and Organization Controls) is a set of criteria for managing and securing sensitive data in service organizations. It is especially important for technology and cloud computing companies, ensuring that data privacy, security, and confidentiality are maintained. More precisely, SOC 2 focuses on five Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type 1 evaluates whether a system is designed properly at a given point in time while SOC 2 Type 2 evaluates that a system is designed and functioning as designed for a given period.
4	**ITIL (Information Technology Infrastructure Library)** [21]	ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business. It covers areas such as incident management, change management, and security management to ensure IT services are delivered effectively and securely.
5	**ISO/IEC 27002** [2]	ISO/IEC 27002 is a comprehensive security standard providing a detailed set of guidelines for implementing information security controls. It complements ISO/IEC 27001 and focuses on the best practices and controls for protecting information assets. The standard includes controls in areas such as access management, risk assessment, incident management, and business continuity.
6	**ISO/IEC 27018** [3]	ISO/IEC 27018 is a privacy standard specifically addressing the protection of personal data in the cloud. It provides guidelines for cloud service providers to ensure that personal data is handled according to privacy principles and regulations.
7	**ISO/IEC 27032** [4]	ISO/IEC 27032 is a guideline for improving cybersecurity, with a focus on collaboration and coordination between stakeholders, including governments, private organizations, and end users. It provides a framework for managing cyber risks and protecting digital assets.
8	**ITGR (IT Governance and Risk)**	IT Governance and Risk (ITGR) frameworks guide organizations in aligning IT management with business goals, focusing on the governance of IT systems, risk management, and compliance with legal and regulatory requirements.

Table 3. Security Assurance Profiles/Criteria, Compliance Standards, and Product Guidelines related to the AERAS pilots

Concluding, in this section, we have provided a detailed analysis of the security assurance landscape relevant to the two pilots of the AERAS project, encompassing both general security assurance schemes and healthcare-specific standards. These schemes, frameworks, and profiles serve as the foundation for developing the CRSA models and CRST training programs by addressing key security, compliance, and risk management requirements. By evaluating these established standards alongside identified threats and security controls within the pilot organizations, the AERAS project ensures that its models and training programs are tailored to meet both sector-specific and organizational cybersecurity needs.

3 Pilot Requirements, Environments, and Training Programmes Specifications

This section provides a comprehensive overview of the cybersecurity requirements, environment architectures, and the associated threat landscapes of the two pilot activities within the AERAS project. The analysis presented in this section serves as the foundation for understanding the unique security challenges faced by each pilot organization. By thoroughly evaluating the unique operation environments of the organizations participating in the two pilots, identifying key infrastructure components, and assessing the specific cybersecurity needs and risks, we established the groundwork for the development of the respective Cyber Range Security Training (CRST) programs and CRSA models (further detailed in Section 0).

The process involved close collaboration with the pilot organizations (UPAT and PAGNI), leveraging detailed infrastructure analysis and feedback collected through questionnaires and stakeholder engagement. This iterative approach ensures that the defined training programs align with the operational contexts, security needs, and emerging threats of the environments of the pilot organizations, paving the way for targeted and effective cybersecurity training strategies.

3.1 AERAS Pilot Environments Specifications and Threats

This subsection explores the unique environment architectures and threat landscapes of the two AERAS pilots, identifying the specific cybersecurity requirements of each organization. By analyzing the operational contexts, infrastructure, and potential vulnerabilities of the participating organizations, we gain the necessary insights to design and develop the CRSA models and CRST training programs tailored to their needs. The environment-specific characteristics and security challenges described here along with the feedback collected from the foreseen stakeholders involved in the pilot scenarios form the foundation for the adaptive CRSA and CRST models and training programmes developed and detailed in later sections.

3.1.1 Pilot 1: Smart Hospital Environment (UPAT)

This subsection details the environment architecture and associated cybersecurity threats of the **Smart Hospital Environment pilot**, conducted at the School of Medicine of the **University of Patras (UPAT)**. The pilot focuses on a sophisticated healthcare ecosystem that integrates diverse systems, including IoT devices, advanced medical systems, image acquisition units (e.g., PET/CT, CTs, SPECT/CTs, Mammography Units, MRI, Ultrasound, etc.), laboratory test result systems, and critical data flows between personnel. This intricate infrastructure is governed by strict security and privacy regulations, ensuring the safety, confidentiality, and integrity of sensitive healthcare data.

The security and privacy requirements for this environment stem from its role in processing and storing vast amounts of highly sensitive personal health information. With approximately 1K patients examined daily, the hospital generates significant volumes of data that must be securely archived and transmitted. These systems are not only mission-critical but must also operate continuously, 24/7, to support patient care. Consequently, they are prime targets for cyber threats, requiring robust measures to protect against **unauthorized access**, **data breaches**, and **operational disruptions**.

Figure *1* below presents a high-level network diagram illustrating the primary settings, entities, and infrastructure setup of the UPAT pilot environment. This diagram offers an overview of the interconnected systems, encompassing medical imaging units, radiology systems, data archiving systems, and communication pathways linking hospital personnel working in the different units of the hospital and critical infrastructure components. The representation highlights the complexity of the environment, emphasizing the integration of diverse technologies and the continuous flow of sensitive health data. Understanding this infrastructure is essential for identifying potential vulnerabilities, assessing security requirements, and tailoring the CRSA models and CRST training programs to address the specific needs of this pilot environment.

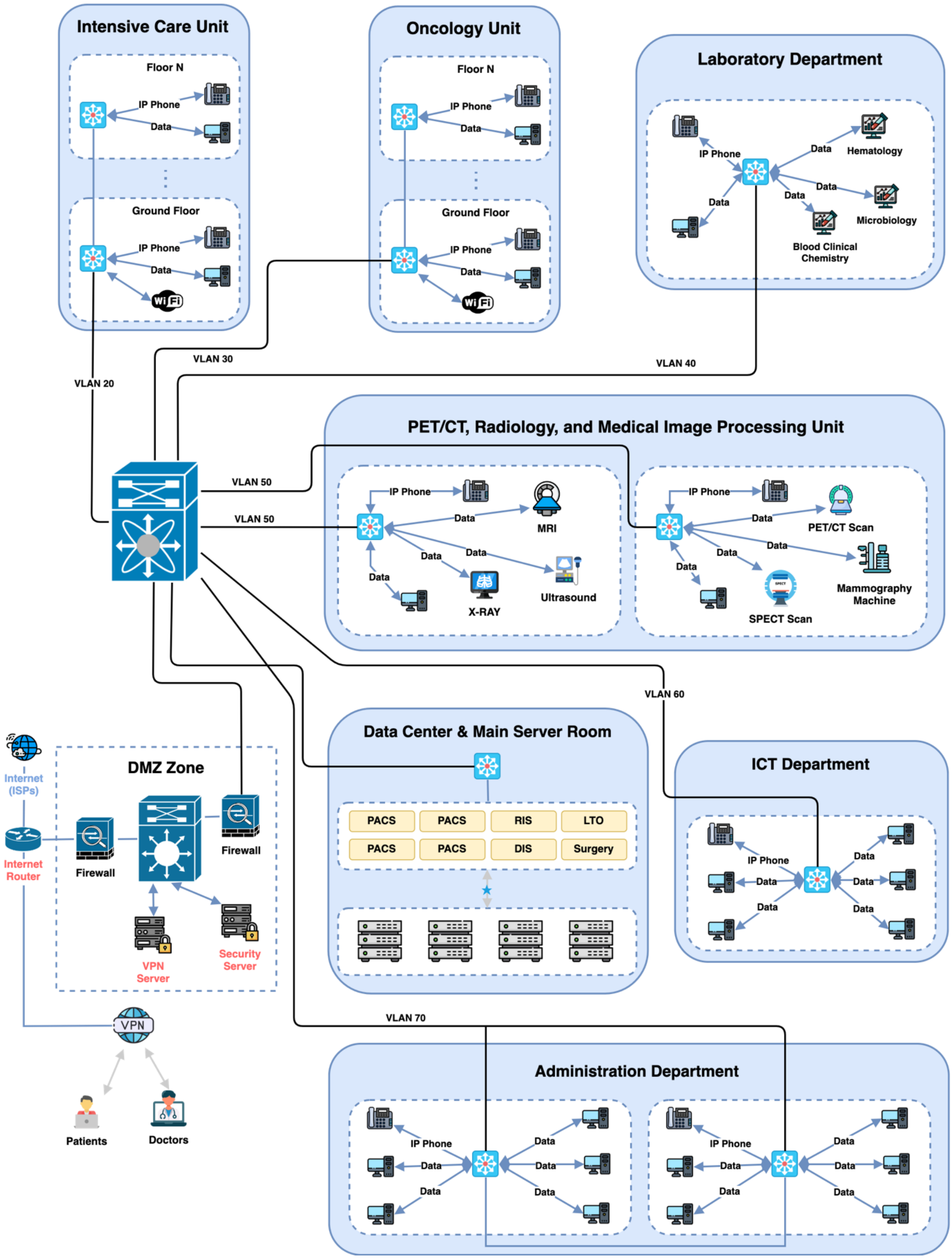

Figure 1. Pilot 1 "Smart Hospital Environment" - UPAT's High-level Network Topology Diagram

As depicted in the high-level network topology diagram above, the Smart Hospital Environment pilot involves a diverse range of stakeholders and actuators, each playing a critical role in the daily operations and overall functionality of the hospital's ecosystem.

Key stakeholders include:

- **End-Users:** This group comprises medical doctors, nurses, administrative personnel, biochemists, and other healthcare professionals who rely on various databases and systems for their daily tasks. These users interact extensively with the infrastructure to access, input, and manage patient data, laboratory results, and imaging records, making them integral to the hospital's workflows.
- **Patients:** Patients are key participants who need secure and reliable access to their examination results and medical records. Their involvement necessitates robust privacy measures to protect sensitive personal and health information.
- **Information Systems:** Various systems operate collaboratively to enable seamless data exchange across the hospital environment. For instance, Picture Archiving and Communication Systems (PACS) interconnect with image acquisition units (e.g., CT scanners, MRI machines) to store and transfer medical images securely and efficiently. These automated systems are crucial for maintaining operational continuity and supporting clinical decision-making.

Furthermore, the hospital personnel represent a critical stakeholder group within the Smart Hospital Environment pilot, as they are directly responsible for managing sensitive patient data and operating complex interconnected system. However, despite their importance, these individuals often face challenges related to their level of security knowledge and practices. Personnel are frequently required to interact with systems they may not fully understand, potentially exposing vulnerabilities through improper use or inadequate awareness of security protocols. In general, their actions and decisions directly impact the security, accuracy, and efficiency of data handling processes.

Key security requirements include ensuring that personnel handle patient data in compliance with privacy regulations, such as GDPR, and adhere to strict policies for secure data storage, access, and transfer. Conversely, vulnerabilities often arise from human errors, such as weak password practices, susceptibility to phishing attacks, or unintentional sharing of sensitive information. These gaps in knowledge and behavior can compromise not only individual systems but also the entire hospital infrastructure. Hence, proper training of personnel is a cornerstone of safeguarding patient data and ensuring the resilience of the hospital's operations.

To address these challenges, a robust awareness and training framework must be established for all personnel. This framework should focus on equipping employees with the knowledge and skills needed to operate securely in a high-risk environment. By fostering a culture of security awareness, the hospital can mitigate vulnerabilities and enhance the overall resilience of its systems.

The framework should cover the following **factors and awareness aspects**:

1. **Understanding System Functionality:** Training personnel to comprehend the systems they use, including their capabilities, limitations, and security features.
2. **Data Handling Practices:** Ensuring secure practices for storing, accessing, and sharing sensitive patient information.
3. **Password Management:** Educating personnel on creating and maintaining strong, unique passwords and recognizing the risks of password reuse.
4. **Phishing and Social Engineering Awareness**: Training employees to identify and respond appropriately to phishing attempts or other forms of social engineering attacks.
5. **Incident Reporting:** Establishing clear protocols for reporting suspicious activities or security incidents to minimize response time and mitigate risks.
6. **Device and Endpoint Security:** Highlighting the importance of securing workstations, mobile devices, and other endpoints connected to the hospital’s network.
7. **Regulatory Compliance:** Providing a thorough understanding of relevant data protection regulations (e.g., GDPR, HIPAA) and their implications for daily operations.

8. **Use of Secure Communication Channels:** Promoting secure communication methods for sharing sensitive information within and outside the organization.
9. **Role-specific Security Practices:** Tailoring training programs to the specific roles and responsibilities of different personnel groups, such as medical staff, IT personnel, and administrative employees.
10. **Awareness of Emerging Threats:** Keeping employees informed about evolving cybersecurity threats and the latest best practices to counter them.

By implementing this comprehensive awareness and training framework, the hospital can empower its personnel to serve as a robust first line of defense against cybersecurity threats. This proactive strategy not only safeguards the organization's critical assets but also ensures compliance with stringent regulations, fostering trust among patients and stakeholders. The unique security requirements and awareness needs identified within this environment establish the foundation for defining the hospital's cybersecurity priorities. They also guide the development of tailored CRSA models and CRST training programs, ensuring these solutions effectively address the specific challenges and vulnerabilities inherent in such a complex and sensitive healthcare setting.

3.1.2 Pilot 2: Healthcare Authority (PAGNI)

This subsection examines the environment architecture and associated cybersecurity threats of the **Healthcare Authority pilot**, conducted at the **Panepistimiako Geniko Nosokomeio Irakleiou (PAGNI)**. While the focus of the AERAS project on the healthcare sector results in some similarities between the pilot environments, the specific challenges faced by each organization and the corresponding training needs for their personnel differ at some degree. These distinctions guide the tailored development of cybersecurity models and training programs for each pilot.

The PAGNI pilot revolves around a healthcare environment supported by an integrated information system that provides a wide array of clinical, administrative, and technical services. These include:

- **Medical-nursing Services (HIS):** Supporting patient management and clinical workflows.
- **Administrative-economic Services (ERP):** Handling hospital operations, finance, and resource planning.
- **Laboratory Services (LIS):** Managing laboratory test processes and results.
- **Medical Imaging Services (RIS/PACS):** Ensuring secure storage and retrieval of medical imaging data.
- **Intensive Treatment Unit Services (Critis):** Enabling the management of critical care patients.
- **Technical Biomedical Services (MASO/POINT):** Overseeing biomedical equipment and technical support.

These systems operate within a complex and interconnected infrastructure, governed by strict security and privacy regulations to protect the integrity, confidentiality, and availability of sensitive healthcare data.

Figure *2* below illustrates the high-level topology diagram of PAGNI's infrastructure, showcasing the primary buildings, department units, and their interconnections. The diagram highlights the interaction between medical imaging systems, data archiving solutions, and communication pathways that link personnel across different hospital buildings and critical infrastructure components. The representation underscores the complexity of PAGNI's environment, emphasizing the integration of diverse technologies and the continuous flow of sensitive health data. As with the first pilot of the AERAS project, understanding this intricate setup is essential for identifying vulnerabilities, evaluating security requirements, and designing CRSA models and CRST training programs that address the specific challenges of this pilot. The focus on systems such as HIS, ERP, and RIS/PACS introduces unique security considerations, which we analyze in the rest of this section.

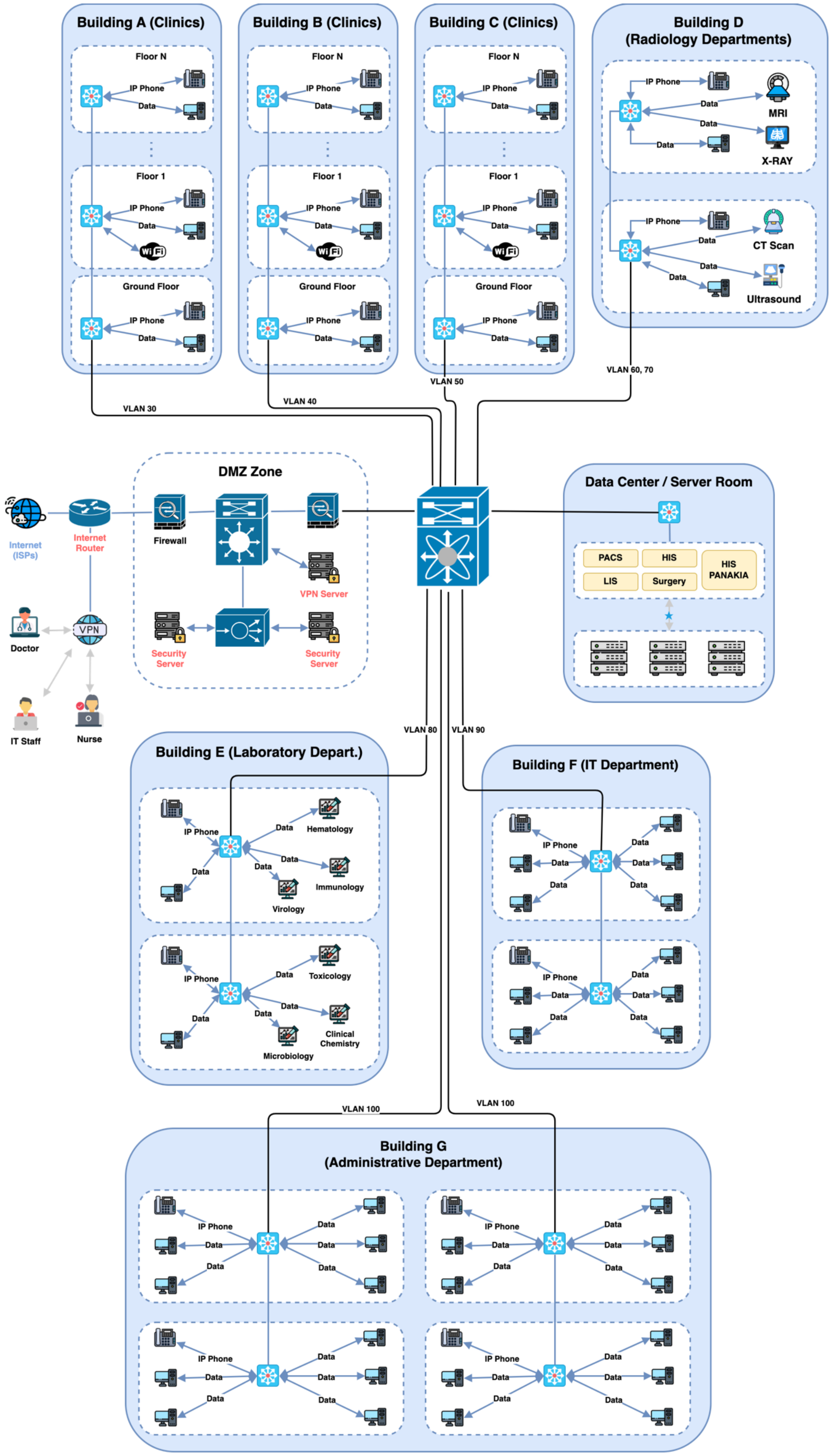

Figure 2. Pilot 2 "Healthcare Authority" - PAGNI's High-level Network Topology Diagram

As depicted in the high-level network topology diagram, the Healthcare Authority pilot involves a diverse array of stakeholders and actuators who are integral to the hospital's daily operations and cybersecurity ecosystem. These stakeholders include:

- **End-users:** Health professionals, such as doctors, nurses, and administrative staff, who routinely interact with PAGNI's systems but often lack specific security or privacy knowledge.
- **PAGNI ICT Personnel:** Specialists responsible for the in-house development and administration of e-health systems, ensuring their functionality and security.
- **Policy Experts:** Personnel with expertise in public health policy, contributing to strategic decisions and operational oversight.

Despite their critical roles, these individuals frequently face challenges in effectively managing the sensitive personal data of patients due to gaps in security knowledge and best practices. Given the volume and sensitivity of the data processed by PAGNI, the hospital is a prime target for cyber-attacks, including phishing, ransomware, and data breaches aimed at unlawfully accessing personal health information. Additionally, disruptions caused by system outages or malware can have far-reaching consequences, affecting not only PAGNI but also its connected network of seven hospitals in Crete, general practitioners, public health centers, the University of Crete, and the 7th Health Region of Crete.

Furthermore, to address these vulnerabilities and threats, the AERAS project must implement such a training framework for the involved stakeholders so that PAGNI can establish and enforce robust security requirements to safeguard its operations and the large volume of sensitive information that it collects and manages daily. Such key cybersecurity requirements include:

1. **Data Protection and Privacy:** Ensuring compliance with regulations like GDPR to protect patient data from unauthorized access or misuse.
2. **System Availability and Resilience:** Maintaining 24/7 availability of critical systems to prevent disruptions that could impact healthcare services.
3. **Secure Interconnectivity:** Safeguarding data exchanges and communications with external entities, such as other hospitals and health centers, to prevent unauthorized access or interception.
4. **Threat Detection and Response:** Implementing advanced monitoring tools and incident response mechanisms to quickly identify and mitigate cyber threats.
5. **Access Control:** Enforcing strict authentication and authorization policies to limit system access to authorized personnel only.
6. **Endpoint Security:** Protecting workstations, medical devices, and other endpoints from vulnerabilities and malware.

To address these challenges effectively, we must implement a comprehensive awareness and training framework for all relevant stakeholders of PAGNI. This framework should promote a culture of security consciousness, ensuring that personnel are well-equipped to navigate and mitigate potential threats. The framework should include the following awareness aspects and training objectives:

1. **Security Fundamentals for End-users:** Educating health professionals about secure practices when interacting with e-health systems, such as proper password management, avoiding phishing traps, and securely handling patient data.
2. **Data Protection and Privacy Awareness:** Ensuring all personnel understand the importance of safeguarding personal health information and complying with GDPR and other relevant regulations.
3. **Threat Landscape Updates:** Keeping stakeholders informed about emerging threats, such as ransomware and social engineering attacks, and how to counter them effectively.
4. **Incident Reporting Protocols:** Teaching personnel how to recognize and report suspicious activities or potential security breaches promptly.

5. **Interconnectivity Security:** Training relevant stakeholders on securely managing data exchanges with external entities to minimize risks associated with interconnected systems.
6. **Advanced Training for ICT Personnel:** Providing in-depth training on system administration, secure configuration, vulnerability management, and incident response.

By targeting to address these requirements, we ensure that the developed CRSA models and the CRST training programs are effective in enhancing the cybersecurity posture of the PAGNI's personnel and its systems. This approach not only mitigates risks but also ensures the hospital can deliver uninterrupted and secure healthcare services, fostering trust among patients and its network of partners.

4 AERAS CRSA-Driven Training Programmes Definitions

This section presents the CRSA-driven Cyber Range Security Training (CRST) scenarios developed for the two pilots of the AERAS project: 1) the Smart Hospital Environment pilot at UPAT; and 2) the Healthcare Authority pilot at PAGNI. Each pilot features three (3) training scenarios designed to address their unique operational environments, cybersecurity requirements, and identified threats. Having such models facilitates interoperability across different training platforms that use cyber ranges, as the models can be readily converted into training activity specifications that can be shared and adapted among them. This concept was previously explored in deliverable D3.3 of the EU-funded H2020 project CONCORDIA [22], where several EU cyber range platforms were analyzed to identify potential mechanisms for exchanging training scenarios effectively.

We note that the selection of the specific training scenarios for each pilot is grounded on three key aspects: (1) the actual cybersecurity requirements and priorities identified for each organization participating in the pilots; (2) an in-depth analysis of the network topology and infrastructure environments of the organizations to pinpoint critical assets and potential vulnerabilities; and (3) crucial feedback gathered from surveys completed by the personnel and pilot participants. These surveys, conducted as part of deliverable D5.3 "AERAS Initial Prototype Pilot Validation Report", provided valuable insights into the cybersecurity awareness levels, training needs, and operational challenges faced by the staff. For a comprehensive discussion of the survey methodology and results, please refer to deliverable D5.3.

Furthermore, for each pilot, we provide an overview of each relevant training scenario, highlighting their objectives and scope, as well as their modelling logic. These scenarios are integral to the iterative validation process of the AERAS platform, ensuring the effectiveness and adaptability of the training programs to real-world cybersecurity challenges.

4.1 Pilot 1: Smart Hospital Environment (UPAT)

This subsection outlines the scenarios for the training programmes developed for the Smart Hospital Environment pilot at UPAT. Three distinct scenarios have been designed to address the specific cybersecurity needs and operational challenges of this healthcare environment:

1. **Identity Spoofing and Unauthorized Access via Phishing Emails:** Targeted at **medical staff, administrative personnel, and other end-users** who access patient data or examination results. This scenario trains participants to recognize and mitigate phishing attaches that exploit email security and user credentials.
2. **Incident Response – Detecting Unauthorized Access to PACS Storage:** Aimed primarily **at IT technical personnel** responsible for managing the hospital's critical systems. This scenario focuses on identifying and responding to unauthorized access attempts to the Picture Archiving and Communication System (PACS) of the hospital, which stores sensitive medical imaging data collected from image acquisition units like the PET/CT, CTs, SPECT/CTs, MRI, Mammography Units, etc.
3. **Denial of Service (DoS) Attack on Hospital Systems:** Designed for **IT staff and administrative personnel** to prepare them for handling disruptions caused by attacks targeting the availability of essential hospital systems, ensuring continuity of operations.

The target audiences for these training scenarios include medical staff such as doctors and nurses, administrative personnel managing operational workflows, end-users accessing patient data and examination results, and IT technical personnel responsible for securing and maintaining hospital systems. By tailoring each scenario to specific roles and responsibilities, the training ensures that all stakeholders are equipped with the knowledge, awareness, and skills necessary to respond effectively to potential cybersecurity threats within the hospital environment.

4.1.1 Scenario 1 - Identity Spoofing and Unauthorized Access via Phishing Emails

This scenario focuses on simulating an identity spoofing attach conducted through phishing emails, where malicious actors attempt to deceive hospital personnel into revealing sensitive credentials or accessing fraudulent links. The training focuses on equipping medical staff, administrative personnel, and other end-users with the skills to recognize and respond to phishing attempts effectively, while understanding the implications of falling victim to such attacks. Participants learn to identify suspicious emails, implement secure practices such as multi-factor authentication, and adopt measures to prevent unauthorized access to the hospital's systems and sensitive data. This scenario highlights the importance of vigilance when interacting with email communication and reinforces secure access control mechanisms.

Relevance to the participating Organization: The hospital processes sensitive health data that must be protected from unauthorized access. Personnel interacting with email are a common target for such attacks, making this scenario critical for training.

4.1.1.1 Scenario Description, Progression, and Learning Objectives

> A member of the administrative staff at a regional hospital receives an email claiming to be from the IT department, requesting immediate action to "validate credentials" due to a supposed system update. The email contains a link to a fake login page resembling the hospital's official portal. The trainee, acting as the target of the phishing attempt, is tasked with identifying suspicious elements in the email and recognizing the signs of a phishing attack.

The scenario begins with the trainee acting as the email recipient, tasked with evaluating the email for suspicious elements, such as unusual sender addresses, grammatical errors, or fake urgency. Upon recognizing the phishing attempt, the trainee must report the email to the IT department and follow proper procedures to ensure no sensitive information is disclosed.

In the progression phase, the simulation escalates to show the potential consequences of a successful phishing attack. If the trainee fails to detect and report the phishing attempt, the scenario simulates unauthorized access to a critical hospital system using compromised credentials. The trainee must then collaborate with IT personnel to investigate the breach, revoke the compromised account, and secure affected systems.

The training concludes by reinforcing best practices, such as enabling multi-factor authentication, verifying suspicious communications through alternative channels, and maintaining vigilance in day-to-day operations.

This scenario is designed to train participants in phishing detection, incident prevention, and response, ensuring they can effectively recognize and mitigate identity spoofing attacks. It utilizes the Assurance and Simulation Tools layers of the AERAS platform to replicate phishing scenarios and incorporates gamification elements to make the learning process interactive and practical.

Scenario Learning Objectives:

- Identify key indicators of phishing attempts.
- Respond appropriately to phishing emails to prevent credential theft.
- Understand and apply secure practices for handling email-based attacks.
- Investigate and mitigate the consequences of unauthorized access following a phishing attack.

4.1.2 Scenario 2 - Incident Response - Detecting Unauthorized Access to PACS Storage

This scenario involves a simulated unauthorized access attempt targeting the hospital's Picture Archiving and Communication System (PACS), which stores sensitive medical imaging data. Designed for IT technical personnel, this training focuses on analyzing system logs, identifying indicators of unauthorized activity, and implementing an effective incident response plan. Participants gain hands-on experience in monitoring, detecting, and mitigating threats to ensure the confidentiality and integrity of medical imaging data within the PACS storage system. This scenario emphasizes the importance of monitoring, auditing, and responding to suspicious activities in systems that handle highly sensitive data.

Relevance to the participating Organization: With daily operations generating vast amounts of imaging data, PACS represents a critical system requiring robust protection. Training personnel to detect and respond to unauthorized access ensures the integrity and confidentiality of stored medical data.

4.1.2.1 Scenario Description, Progression, and Learning Objectives

An IT administrator at the hospital receives a system alert indicating unusual activity in the Picture Archiving and Communication System (PACS) storage. The alert points to repeated access attempts using a compromised user account to retrieve a large volume of medical imaging data. The trainee is tasked with investigating the logs and identifying the source of the breach.

The scenario begins with the trainee accessing the PACS system logs to investigate the alert. The trainee must analyze timestamps, IP addresses, and access patterns to confirm unauthorized access and identify the compromised account. Upon verifying the breach, the trainee is tasked with implementing immediate containment measures, including revoking access to the compromised account and blocking suspicious network traffic.

In the progression phase, the simulation escalates by introducing additional challenges, such as identifying other potentially compromised accounts or tracing the origin of the breach. The trainee collaborates with team members to secure the PACS system, document the findings, and recommend improvements to authentication and monitoring mechanisms.

The scenario concludes with a debriefing session to reinforce lessons learned and provide an overview of best practices for incident detection, investigation, and response. Emphasis is placed on ensuring the integrity and confidentiality of sensitive medical data while minimizing system downtime during such events.

This scenario is designed to train IT technical personnel in handling incidents involving unauthorized access to critical healthcare systems. The training utilizes the Assurance and Simulation Tools layers of the AERAS platform to replicate real-world PACS environments and integrates gamification elements to make the learning process interactive and engaging.

Scenario Learning Objectives:

- Analyze system logs to identify signs of unauthorized access.
- Implement effective containment measures to secure compromised systems.
- Collaborate with team members to investigate and resolve security incidents.
- Strengthen monitoring and authentication protocols to prevent future breaches.

4.1.3 Scenario 3 - Denial of Service (DDos) Attack on Hospital Systems

This scenario addresses the risk of a Denial of Service (DoS) attack, where attackers disrupt the availability of critical hospital systems, including patient record management or laboratory information systems. The training is tailored for IT staff and administrative personnel, equipping them with the ability to identify early warning signs of a DoS attack, implement mitigation strategies, and activate backup protocols to maintain service continuity. This scenario emphasizes the importance of operational resilience in a healthcare setting that requires 24/7 system availability.

Relevance to the participating Organization: UPAT relies on 24/7 availability of its systems to manage patient care effectively. A DoS attack could severely hinder operations, making it vital for personnel to understand and respond to such threats promptly.

4.1.3.1 Scenario Description, Progression, and Learning Objectives

> The hospital's IT department detects an unusual spike in network traffic directed at its central patient record management system, causing significant performance degradation. This simulated Distributed Denial of Service (DDoS) attack is designed to disrupt the availability of critical hospital systems, potentially impacting patient care and administrative operations.

The scenario begins with the trainee, acting as an IT administrator, detecting early warning signs of a potential DDoS attack through abnormal traffic patterns and system performance degradation. The trainee must identify and isolate the malicious traffic by analyzing network logs, recognizing suspicious IP addresses, and determining the scale of the attack.

In the progression phase, the simulation escalates, mimicking the impact of the attack on multiple systems and hospital departments. The trainee is tasked with implementing mitigation strategies, including activating traffic filtering mechanisms, redistributing load through load balancing, and applying rate-limiting rules to reduce the attack’s effectiveness. In parallel, the trainee must ensure backup protocols are activated to maintain service continuity for critical systems, minimizing disruptions to hospital operations.

As the attack subsides, the trainee collaborates with the IT security team to conduct a root cause analysis, documenting the nature of the attack, its origin, and the countermeasures employed. The scenario concludes by focusing on preventive measures, such as updating firewall configurations, deploying intrusion detection and prevention systems (IDPS), and reinforcing the network’s overall resilience.

This scenario is designed to train IT personnel and administrative staff in recognizing, mitigating, and recovering from large-scale network-based attacks, ensuring the uninterrupted operation of essential hospital systems. The training leverages the Assurance and Simulation Tools layers of the AERAS platform to replicate realistic DDoS attack conditions and incorporates gamification elements to provide hands-on, interactive learning.

Scenario Learning Objectives:

- Detect early signs of DDos attack through traffic analysis.
- Apply mitigation strategies to reduce the impact of the attack on critical hospital systems.
- Activate and manage backup protocols to ensure service continuity during an attack.
- Conduct root cause analysis and implement preventive measures to strengthen network resilience.

4.2 Pilot 2: Healthcare Authority (PAGNI)

This subsection presents the training programme scenarios designed for the Healthcare Authority pilot at PAGNI. These scenarios are tailored to address the unique cybersecurity challenges and operational needs of PAGNI, focusing on threats that could disrupt critical systems or compromise sensitive healthcare data.

The three scenarios focus on distinct threats and training needs:

1. **Social Engineering:** Educates personnel on recognizing and mitigating manipulation tactics used by attackers to extract sensitive information.
2. **Ransomware Attack on Critical Systems:** Equips IT staff to detect, isolate, and recover from ransomware attacks that target sensitive healthcare data and disrupt of essential operations.
3. **System Configuration and Secure Healthcare Services:** Trains IT personnel in securing system configurations to ensure the availability, confidentiality, and integrity of critical healthcare services.

The target audiences for these scenarios include health professionals, administrative staff, IT technical personnel, and public health policy specialists, with each training scenario designed to address the specific roles and responsibilities of these stakeholders. The training incorporates tools from the Assurance and Cyber Range Tools layers of the AERAS platform, enhanced by gamification elements to deliver interactive and practical learning experiences.

4.2.1 Scenario 1 - Social Engineering

This scenario focuses on the risk of social engineering attacks, where attackers exploit human psychology to manipulate hospital personnel into divulging sensitive information or granting unauthorized access. Examples include impersonating IT staff or trusted partners to extract login credentials or patient data. The training is tailored for administrative staff, health professionals, and IT personnel, equipping them with the skills to recognize manipulative tactics, validate requests, and adhere to organizational security policies.

Relevance to the participating Organization: PAGNI handles vast amounts of sensitive patient data daily, making it a prime target for attackers leveraging social engineering techniques. A successful attack could lead to unauthorized access to critical systems, emphasizing the need for personnel to understand and mitigate these threats effectively.

4.2.1.1 Scenario Description, Progression, and Learning Objectives

This scenario simulates a social engineering attack, where an attacker contacts hospital personnel, impersonating a trusted entity such as the IT department or a partner organization, to extract sensitive information or gain unauthorized access. For instance, the attacker may request login credentials under the guise of “performing urgent system maintenance.

The trainee, acting as a hospital staff member, must recognize the manipulative tactics used by the attacker, such as creating a sense of urgency, using technical jargon, or leveraging personal trust. The first phase involves identifying the suspicious behavior during the interaction and refusing to provide sensitive information.

In the progression phase, the attacker employs more sophisticated techniques, such as providing seemingly legitimate documentation or escalating the urgency of the request. The trainee must validate the request by following organizational protocols, such as verifying identities through official channels and reporting the incident to IT security teams.

The scenario concludes with a debriefing that emphasizes the importance of organizational security policies, awareness of social engineering tactics, and effective reporting mechanisms.

Scenario Learning Objectives:

- Recognize and respond to common social engineering tactics.
- Validate the authenticity of requests for sensitive information.
- Understand the importance of organizational security policies and reporting mechanisms.

4.2.2 Scenario 2 - Ransomware Attack on Critical Systems

This scenario addresses the risk of a ransomware attack, where malicious actors encrypt critical healthcare data and demand payment to restore access. Such attacks can severely disrupt hospital operations, affecting patient care and administrative workflows. The training is tailored for IT personnel and administrative staff, preparing them to identify early signs of ransomware, isolate affected systems, and implement recovery strategies using secure backups.

Relevance to the participating Organization: PAGNI's reliance on interconnected systems and sensitive healthcare data makes it a high-value target for ransomware attacks. A ransomware incident could disrupt critical services and compromise patient safety, highlighting the importance of training personnel to detect, respond to, and recover from such attacks.

4.2.2.1 Scenario Description, Progression, and Learning Objectives

This scenario simulates a ransomware attack targeting PAGNI's critical systems, such as the Hospital Information System (HIS) or Laboratory Information System (LIS), with the goal of encrypting sensitive healthcare data and disrupting essential operations. The attacker demands payment to restore access to the affected systems, placing immense pressure on the hospital's IT and administrative teams.

The scenario begins with the trainee, acting as an IT administrator, identifying early indicators of a ransomware attack, such as unusual file extensions, unexpected encryption activity, or ransom messages appearing on user terminals. The trainee must act quickly to isolate the affected systems to prevent further spread of the ransomware across the network.

In the progression phase, the simulation escalates by introducing complications, such as backup systems being partially impacted or delays in identifying the initial point of entry (e.g., through phishing emails or unpatched vulnerabilities). The trainee must implement mitigation steps, including restoring systems from unaffected backups, identifying the origin of the attack, and ensuring infected systems are removed from the network.

The scenario concludes with the trainee preparing a post-incident report detailing the attack's scope, impact, and the steps taken to mitigate it. The report should also include recommendations for improving ransomware defenses, such as implementing regular offline backups, patch management, and employee training on recognizing phishing attempts.

Scenario Learning Objectives:

- Detect early signs of ransomware attacks on critical systems.
- Isolate affected systems to contain the spread of ransomware.
- Restore operations using secure backups while ensuring minimal downtime.
- Analyze the root cause of the attack and recommend long-term preventive measures.

This scenario is designed to prepare IT personnel and administrative staff to handle ransomware incidents effectively, ensuring the hospital can quickly recover from attacks without compromising sensitive data or critical services. The training utilizes the Assurance and Simulation Tools layers of the AERAS platform, integrating gamification elements to enhance engagement and learning through hands-on exercises.

4.2.3 Scenario 3 - System Configuration and Secure Healthcare Services

This scenario highlights the importance of secure system configurations in protecting healthcare services and ensuring compliance with privacy regulations. It focuses on identifying and resolving misconfigurations, such as default credentials or weak access controls, that could expose critical systems to attacks. The training is tailored for IT personnel, equipping them with the skills to maintain secure configurations and respond to threats targeting system vulnerabilities.

Relevance to the participating Organization: PAGNI depends on securely configured systems to ensure the confidentiality, integrity, and availability of healthcare services. Misconfigurations represent a significant risk, potentially allowing attackers to exploit vulnerabilities. Training IT personnel to proactively secure systems are critical to protecting PAGNI's infrastructure and sensitive patient data.

4.2.3.1 Scenario Description, Progression, and Learning Objectives

This scenario addresses the critical need for secure system configurations to protect healthcare services and sensitive patient data. The trainee, acting as a system administrator, is tasked with securing the configuration of PAGNI's Laboratory Information System (LIS) after detecting vulnerabilities that could be exploited to gain unauthorized access.

The scenario begins with the trainee analyzing a security audit report that highlights misconfigurations, such as default credentials, unnecessary open ports, and weak access control policies. The trainee must identify and resolve these issues to ensure compliance with security policies and standards.

In the progression phase, the simulation introduces additional challenges, such as the system being actively targeted by attackers exploiting unpatched vulnerabilities. The trainee must prioritize fixes, implement software updates, and reinforce access controls while ensuring minimal disruption to ongoing operations.

The scenario concludes with a focus on preventive measures, including regular system audits, employee training on secure practices, and adopting a zero-trust architecture to protect critical healthcare services.

Scenario Learning Objectives:

- Identify and resolve misconfigurations in healthcare systems.
- Apply secure practices for system configuration and access controls.
- Respond to active threats while maintaining system availability and integrity.
- Establish preventive measures to ensure long-term security.

5 AERAS CRSA-Driven Cyber Range Programmes Specification

In this section, we present the first version of the defined and developed Cyber Range Security Assurance (CRSA) models, including their sub-models, and the Cyber Range Simulation and Training (CRST) programs specifications. These have been tailored for the training scenarios of the two pilots in the AERAS project. The section includes all relevant details and outlines the development procedures that enable the dynamic adaptation of the CRSA models to meet the evolving security needs of the pilot environments.

It is important to note that the defined Cyber Range training programs and models presented here represent an initial iteration. These will be further refined and enhanced throughout the upcoming months, as the pilots are evaluated, and feedback is incorporated. The final version of the training programs and models will be detailed in Deliverable D3.3: AERAS Models and CRSA-driven Cyber Range Programme V2, which is scheduled for submission in Month 66 of the project.

The definition, development, and setup of the Cyber Range Programmes and their sub-models followed a structured, multi-step process.

- **Step 1 - Pilot Environment Architecture and Core Assets Analysis:** This initial phase involves an in-depth analysis of the pilot systems to identify their core assets and existing threats.
- **Step 2 - Pilot Environments Threats and Security Requirements Analysis:** Building on the findings of Step 1, this phase focuses on identifying the specific threats and cybersecurity requirements of each pilot.
- **Step 3 - Cyber Range Security Assurance (CRSA) Model Definition and Creation:** Leveraging the insights from Step 1 and 2, the core CRSA model was defined and created to represent the security assurance needs of the pilot environments.
- **Step 4 - Creation of Cyber Range Security Assurance Sub-models:** During this phase, sub-models of the CRSA were developed to address specific components and scenarios within the pilot environments.
- **Step 5 - Definition and Creation of the Cyber Range Simulation and Training (CRST) Model:** In this final phase, the CRST models and training programs were designed and initiated for all the scenarios defined in Section 0, ensuring alignment with the pilots' operational contexts and security objectives.

The development of the CRSA and CRST models is grounded in the language and framework defined in Deliverable D3.1: CRSA Models and CRSA-driven Cyber Range Programme Specification Language. The CRSA model, along with its sub-models, primarily serves to describe an organization’s infrastructure while specifying potential threats and vulnerabilities associated with the software and hardware components of that infrastructure. These models provide a structured approach to understanding the security posture of an organization and identifying areas requiring targeted mitigation and assurance.

On the other hand, a CRST model is designed to define specific training programs aligned with the identified cybersecurity requirements, threats, and operational needs of the organization. Each developed CRST model is tailored to the scenarios defined in Section 0, offering practical training to address real-world challenges.

In the following subsections, we provide the CRSA models developed for the infrastructures of the two pilot organizations, detailing how they address the specific needs of each environment. Additionally, we also present the Cyber Range Simulation and Training Programme (CRST) models developed for the training scenarios of each pilot. These examples showcase the structure, objectives, and methodology behind the developed training programs, providing insight into their implementation.

5.1 Pilot 1: Smart Hospital Environment (UPAT)

5.1.1 Overview

This section provides an in-depth exploration of the CRSA models developed for the Smart Hospital Environment pilot at UPAT. The CRSA models describe the hospital's infrastructure, including its core assets, potential threats, and vulnerabilities, forming a comprehensive framework for assessing and enhancing the organization’s cybersecurity posture. These models are continuously utilized by the Cyber System Continuous Monitoring Aggregator layer of the AERAS platform architecture to monitor the infrastructure in real-time.

The Cyber System Continuous Monitoring Aggregator layer not only evaluates the hospital's ongoing security landscape but also correlates the results of the cyber range training programs with changes in the organization’s overall security posture. This feedback loop ensures that the effectiveness of the training programs is validated against actual improvements in security, allowing for dynamic adaptations to the existing CRSA models as required.

Additionally, we detail the CRST models for all the three scenarios of this pilot. This training program provides an actionable and practical approach to equipping hospital personnel with the skills necessary to address one of the most prevalent cybersecurity threats in the healthcare sector.

Together, the CRSA models and CRST training programs, supported by the continuous monitoring capabilities of the AERAS platform, exemplify the adaptive and comprehensive methodology employed to meet the unique cybersecurity needs of the UPAT pilot.

Please note that, any names and personal information presented in this document are entirely artificial. Out of respect for the privacy of individuals and in adherence to data protection regulations, we have not included real information about the persons involved in each pilot. These artificial examples are provided solely for illustrative purposes to demonstrate the roles and responsibilities within the modelled framework.

5.1.2 Cyber Range Security Assurance (CRSA) Models

The CRSA Model and its sub-models for the first pilot, specified using the defined language, are presented below:

```
SecurityAssurance(
    name("UPAT_Security_Assurance_Model"),
    dateFrom("2024-09-14"),
    dateTo(null),  // Represents that it is currently active
    description("This is the foundational security assurance model for UPAT's Smart Hospital Environment. It
serves as the superclass for all other elements, including threats, assets, and vulnerabilities."),
    creator(Person(
        firstName("Maria"),
        lastName("Papadopoulou"),
        organisation("University of Patras"),
        description("Head of IT Security overseeing cybersecurity and compliance at UPAT."),
        roles(security_manager)
    )),
    status("draft") // Will be marked final when all OCL constraints are met
)
```

```
Vulnerability(
    name("Unpatched_Medical_Imaging_Software"),
    source("National Vulnerability Database (NVD)"),
    publishedDate("2024-09-15"),
    lastModified("2024-09-15"),
    vulnerabilityType("Computational"),
    description("The medical imaging software running on the PACS system is outdated and contains unpatched vulnerabilities that could allow remote attackers to execute arbitrary code."),
    mitigatedBy(SecurityControl(name("Patch_Management_Program"))),
    appliesTo(Asset(name("PACS_Server"), assetType("Software"))),
    canBeExploitedBy(Violation(name("Unauthorized_Access"))),
    couldLeadToViolationOf(SecurityProperty(name("Confidentiality")))
)

Vulnerability(
    name("Weak_Password_Policies"),
    source("Internal IT Audit Report"),
    publishedDate("2024-09-15"),
    lastModified("2024-09-15"),
    vulnerabilityType("Computational"),
    description("Administrative accounts on the PACS and laboratory systems have weak password requirements, making them vulnerable to brute force or dictionary attacks."),
    mitigatedBy(SecurityControl(name("Enforced_Password_Policies"))),
    appliesTo(Asset(name("Administrative_Accounts"), assetType("Person"))),
    canBeExploitedBy(Violation(name("Identity_Spoofing"))),
    couldLeadToViolationOf(SecurityProperty(name("Integrity")))
)

Vulnerability(
    name("Unsecured_WiFi_Access_Points"),
    source("Penetration Testing Report"),
    publishedDate("2024-09-15"),
    lastModified("2024-09-15"),
    vulnerabilityType("Physical"),
    description("Wi-Fi access points in the Oncology Unit are unsecured, allowing unauthorized devices to connect and potentially intercept sensitive patient data."),
    mitigatedBy(SecurityControl(name("WPA3_Encryption_and_MAC_Filtering"))),
    appliesTo(Asset(name("Oncology_Unit_WiFi"), assetType("Network"))),
    canBeExploitedBy(Violation(name("Man-in-the-Middle_Attack"))),
    couldLeadToViolationOf(SecurityProperty(name("Confidentiality")))
)
```

```
Threat(
    name("Phishing_Attack"),
    likelihood("High"),
    source("ENISA Threat Landscape Report 2024"),
    category("Social Engineering"),
    description("A phishing attack aimed at administrative staff to steal credentials and gain unauthorized access to the PACS system or other sensitive resources."),
    mayViolate(SecurityProperty(name("Confidentiality"))),
    mayViolate(SecurityProperty(name("Integrity")))
)

Threat(
    name("Unauthorized_Access_to_PACS"),
    likelihood("Medium"),
    source("Internal Risk Assessment Report"),
    category("Insider Threat"),
   description("An unauthorized access attempt targeting the PACS storage system to extract sensitive
medical imaging data."),
   mayViolate(SecurityProperty(name("Confidentiality"))),
   mayViolate(SecurityProperty(name("Availability")))
)

Threat(
   name("DDoS_Attack"),
   likelihood("Medium"),
   source("ENISA Threat Landscape Report 2023"),
   category("Computational"),
   description("A Distributed Denial of Service (DDoS) attack targeting critical hospital systems, such as the
patient record management system, to disrupt availability."),
   mayViolate(SecurityProperty(name("Availability")))
)
```

```
Asset(
   name("PACS_Server"),
   value("€50,000"),
   description("The PACS server manages and stores critical medical imaging data such as X-rays, CT scans, and
MRIs."),
   vendor("GE Healthcare"),
   version("v5.6.2"),
   operatesIn(true),
   managedBy(Asset(name("Data_Center"))),
   protectedBy(SecurityControl(name("Firewall"))),
   communicatesThrough(Asset(name("Hospital_Network")))
)

Asset(
   name("RIS_Server"),
   value("€40,000"),
   description("The RIS server supports workflows and manages radiology department data, ensuring accurate
imaging reports."),
   vendor("Siemens Healthineers"),
   version("v3.4.5"),
   operatesIn(true),
   managedBy(Asset(name("ICT_Department"))),
   protectedBy(SecurityControl(name("Network Access Control"))),
   communicatesThrough(Asset(name("Hospital_Network")))
)

Asset(
   name("Laboratory_Information_System"),
   value("€30,000"),
   description("Manages laboratory workflows, including test results, patient data, and laboratory
operations."),
   vendor("Abbott Laboratories"),
   version("v2.7.1"),
   operatesIn(true),
   managedBy(Asset(name("ICT_Department"))),
   protectedBy(SecurityControl(name("Encryption and Data Backup"))),
   communicatesThrough(Asset(name("Laboratory_Department_Network")))
)
```

```
Asset(
   name("Data_Center"),
   value("€200,000"),
   description("The centralized facility housing the hospital's servers, including PACS, RIS, and LIS."),
   physicalType("Facility"),
   contains(Asset(name("PACS_Server"))),
   contains(Asset(name("RIS_Server"))),
   contains(Asset(name("Laboratory_Information_System"))),
   protectedBy(SecurityControl(name("Physical Access Control"))),
   communicatesThrough(Asset(name("Hospital_Network")))
)

Asset(
   name("DMZ_Zone"),
   value("€30,000"),
   description("A demilitarized zone facilitating secure communication with external users and systems."),
   physicalType("Network_Segment"),
   contains(Asset(name("Firewall"))),
   contains(Asset(name("VPN_Server"))),
   protectedBy(SecurityControl(name("Network Firewall"))),
   communicatesThrough(Asset(name("Internet_Router")))
)

Asset(
   name("ICU_Network"),
   value("€15,000"),
   description("The network segment dedicated to the Intensive Care Unit, connecting patient monitoring
systems and staff communication tools."),
   physicalType("VLAN"),
   communicatesThrough(Asset(name("Hospital_Network")))
)

Asset(
   name("Administrative_Network"),
   value("€10,000"),
   description("The network segment connecting administrative systems and staff computers for hospital
management tasks."),
   physicalType("VLAN"),
   communicatesThrough(Asset(name("Hospital_Network")))
)

Asset(
   name("Patient_Records_Database"),
   value("€500,000"),
   description("A central repository containing sensitive patient information, including medical histories and
diagnostic results."),
   protectedBy(SecurityControl(name("Data Encryption"))),
   isContainedIn(Asset(name("Data_Center"))),
   communicatesThrough(Asset(name("Hospital_Network")))
)
```

```
SoftwareAsset(
   name("PACS_Software"),
   level("SAL"),  // Application Layer Software
```

```
  description("The PACS (Picture Archiving and Communication System) software manages, stores, and retrieves medical imaging files, enabling efficient workflow in the radiology department."),
  provides(Interface(name("ImageDataAPI"))),
  requires(Interface(name("DatabaseCommunicationAPI"))),
  providesImplTo(InterfaceImp(
    impType("REST"),
    accessEndPoint("https://pacs.upat.gr/api"),
    codeFile("/opt/pacs/api/image_data_rest_impl.java")
  ))
)

SoftwareAsset(
  name("LIS_Software"),
  level("SAL"),  // Application Layer Software
  description("The LIS software manages laboratory workflows, including test results, patient data, and sample processing."),
  provides(Interface(name("LabResultsAPI"))),
  requires(Interface(name("PatientDataInterface"))),
  providesImplTo(InterfaceImp(
    impType("REST"),
    accessEndPoint("https://lis.upat.gr/api"),
    codeFile("/opt/lis/api/lab_results_rest_impl.java")
  ))
)

SoftwareAsset(
  name("VMware_Platform"),
  level("PAL"),  // Platform Layer Software
  description("A VMware-based virtual platform used to host and manage critical hospital services, including PACS, LIS, and RIS."),
  provides(Interface(name("VMManagementAPI"))),
  requires(Interface(name("SystemMonitoringInterface"))),
  providesImplTo(InterfaceImp(
    impType("Internal"),
    codeFile("/usr/vmware/internal_vm_management_api.java")
  ))
)

Interface(
  name("ImageDataAPI"),
  isProvidedBy(SoftwareAsset(name("PACS_Software"))),
  isRequiredBy(SoftwareAsset(name("LIS_Software"))),
  isImplementedBy(InterfaceImp(
    impType("REST"),
    accessEndPoint("https://pacs.upat.gr/api"),
    codeFile("/opt/pacs/api/image_data_rest_impl.java")
  ))
)

Interface(
  name("LabResultsAPI"),
  isProvidedBy(SoftwareAsset(name("LIS_Software"))),
  isRequiredBy(SoftwareAsset(name("PACS_Software"))),
  isImplementedBy(InterfaceImp(
    impType("REST"),
    accessEndPoint("https://lis.upat.gr/api"),
        codeFile("/opt/lis/api/lab_results_rest_impl.java")
    ))
)
```

```
HardwareAsset(
    name("PACS_Server"),
    hwType("Computational"),
    description("A physical server used to manage and store medical imaging data, such as X-rays, MRIs, and CT scans."),
    hasSubmodule(MemoryModule(
        noOfModules("4"),
        memorySize("16GB"),
        memoryType("DDR4"),
        memorySpeed("3200 MHz"),
        memoryManufacturer("Corsair")
    )),
    hasSubmodule(DriveModule(
        driveLocation("Internal"),
        noOfDrives("4"),
        driveController("RAID Controller"),
        driveFirmware("v3.2.1"),
        driveCapacity("2TB each")
    )),
    hasSubmodule(CPUModule(
        processorName("Intel Xeon Gold 6248"),
        numberOfCores("20"),
        numberOfThreads("40"),
        processorBaseFrequency("2.5 GHz"),
        socket("LGA 3647")
    )),
    hasSubmodule(BiosModule(
        sysBiosVersion("2.1.0"),
        biosDate("2022-05-15")
    )),
    isPartOf(HardwareAsset(name("Data_Center")))
)

HardwareAsset(
    name("Firewall_DMZ"),
    hwType("Network"),
    description("A physical firewall appliance providing network protection for external communication through the DMZ Zone."),
    hasSubmodule(PortModule(
        ioPort("Ethernet"),
        isAlwaysConnected("True")
    )),
    hasSubmodule(PortModule(
        ioPort("USB"),
        isAlwaysConnected("False")
    )),
    isPartOf(HardwareAsset(name("DMZ_Zone")))
)

HardwareAsset(
    name("MRI_Scanner"),
    hwType("Medical Device"),
    description("A high-resolution MRI scanner used in the radiology department for diagnostic imaging."),
    hasSubmodule(DriveModule(
        driveLocation("Internal"),
        noOfDrives("2"),
        driveController("SCSI Controller"),
        driveFirmware("v5.4.0"),
        driveCapacity("1TB each")
    )),
    hasSubmodule(CPUModule(
        processorName("AMD EPYC 7742"),
        numberOfCores("64"),
        numberOfThreads("128"),
        processorBaseFrequency("2.25 GHz"),
        socket("SP3")
    )),
    isPartOf(HardwareAsset(name("PET/CT_Radiology_Unit")))
)

HardwareAsset(
    name("Switch_Oncology_Unit"),
    hwType("Network"),
    description("A network switch enabling communication and data exchange within the Oncology Unit."),
    hasSubmodule(PortModule(
        ioPort("Ethernet"),
        isAlwaysConnected("True")
    )),
    isPartOf(HardwareAsset(name("Oncology_Unit")))
)
```

```
DataAsset(
  name("Patient_Records_Database"),
  dataType("Operational"),
  dataState("At_Rest"),
  description("A central repository containing sensitive patient health records, including diagnostic results,
medical histories, and treatment plans."),
  storageLocation(Asset(name("PACS_Server"))),
  accessControls(SecurityControl(name("Role-Based Access Control"))),
  encryptionStatus("Enabled (AES-256)"),
  classification("Confidential")
)

DataAsset(
  name("Lab_Test_Results_Data"),
  dataType("Operational"),
  dataState("In_Processing"),
  description("Laboratory test results, such as blood work and chemical analysis, processed and managed by
the LIS."),
  storageLocation(Asset(name("Laboratory_Information_System"))),
  accessControls(SecurityControl(name("Access Control List (ACL)"))),
  encryptionStatus("Enabled (SSL/TLS)"),
  classification("Sensitive")
)

DataAsset(
  name("Network_Configuration_Files"),
  dataType("Configuration"),
  dataState("At_Rest"),
  description("Configuration files for network devices, including VLAN assignments, routing tables, and
firewall rules.")
  storageLocation(Asset(name("ICT_Department_Server"))),
  accessControls(SecurityControl(name("Admin-Only Access"))),
  encryptionStatus("Enabled"),
  classification("Security")
)

DataAsset(
  name("Administrative_Records"),
  dataType("Admin"),
  dataState("At_Rest"),
  description("Records of hospital administrative activities, including payroll, scheduling, and human
resources data."),
  storageLocation(Asset(name("Administrative_Network"))),
  accessControls(SecurityControl(name("Multi-Factor Authentication"))),
  encryptionStatus("Enabled (AES-256)"),
  classification("Confidential")
)
```

```
Person(
   name("Maria"),
   surname("Papadopoulou"),
   dateOfBirth("YYYY-MM-DD"),
   role("Asset Owner"),
   description("Head of IT Security at UPAT, responsible for overseeing the security of all computational and
data assets within the organization."),
   associatedAssets([
      Asset(name("PACS_Server")),
      Asset(name("Patient_Records_Database")),
      Asset(name("Administrative_Records"))
   ])
)

Person(
   name("Ioannis"),
   surname("Dimitriou"),
   dateOfBirth("YYYY-MM-DD"),
   role("Asset Controller"),
   description("IT Security Specialist responsible for managing security measures and ensuring the integrity
and availability of critical systems like PACS and LIS."),
   associatedAssets([
      Asset(name("Laboratory_Information_System")),
      Asset(name("Network_Configuration_Files"))
   ])
)

Person(
   name("xxxx"),
   surname("xxxx"),
   dateOfBirth("YYYY-MM-DD"),
   role("System Administrator"),
  description("Network Administrator overseeing the hospital's VLANs, network devices, and ensuring
connectivity across all units."),
  associatedAssets([
    Asset(name("ICU_Network")),
    Asset(name("Administrative_Network")),
    Asset(name("Firewall_DMZ"))
  ])
)

Person(
  name("xxxx"),
  surname("xxxx"),
  dateOfBirth("YYYY-MM-DD"),
  role("End-User"),
  description("Radiologist utilizing PACS and imaging systems to analyze and diagnose patient conditions."),
  associatedAssets([
    Asset(name("PACS_Software")),
    Asset(name("MRI_Scanner"))
  ])
)
```

```
NetworkAsset(
  name("ICU_VLAN_20"),
  connectedThrough("Ethernet"),
  description("A network segment dedicated to the Intensive Care Unit, facilitating secure data exchange
between patient monitoring devices and hospital systems."),
  associatedHardware([
    HardwareAsset(name("Switch_Intensive_Care")),
    HardwareAsset(name("Firewall_DMZ"))
  ])
)

NetworkAsset(
  name("Oncology_Unit_VLAN_30"),
  connectedThrough("Wi-Fi"),
  description("A network segment for the Oncology Unit, connecting communication devices and facilitating
data transfer between floors."),
  associatedHardware([
    HardwareAsset(name("Wi-Fi_Router_Oncology")),
    HardwareAsset(name("Switch_Oncology_Unit"))
  ])
)

NetworkAsset(
  name("Laboratory_VLAN_40"),
  connectedThrough("Ethernet "),
  description("A VLAN segment for the Laboratory Department, ensuring secure communication for LIS and
other laboratory systems."),
  associatedHardware([
    HardwareAsset(name("Switch_Laboratory"))
  ])
)

NetworkAsset(
  name("Radiology_And_Medical_Imaging_Network_VLAN_50"),
  connectedThrough("Ethernet"),
  description("A dedicated network segment for the PET/CT, Radiology, and Medical Image Processing Unit, supporting secure data transmission between imaging devices, IP phones, and connected systems."),
  associatedHardware([
    HardwareAsset(name("Switch_Radiology_Unit")),
    HardwareAsset(name("MRI_Device")),
    HardwareAsset(name("Ultrasound_Device")),
    HardwareAsset(name("X-Ray_Machine")),
    HardwareAsset(name("PET_CT_Scanner")),
    HardwareAsset(name("SPECT_Scanner")),
    HardwareAsset(name("Mammography_Machine"))
  ])
)

NetworkAsset(
  name("ICT_Department_VLAN_60"),
  connectedThrough("Ethernet"),
  description("A dedicated VLAN for the ICT Department, supporting secure data exchange for IT systems and administrative operations."),
  associatedHardware([
    HardwareAsset(name("Switch_IT_Department")),
    HardwareAsset(name("Firewall_DMZ"))
  ])
)

NetworkAsset(
  name("Administrative_Network_VLAN_70"),
  connectedThrough("Ethernet"),
  description("The network segment supporting administrative systems, connecting computers and communication devices in the Administration Department."),
  associatedHardware([
    HardwareAsset(name("Switch_Administration_Department")),
    HardwareAsset(name("Firewall_DMZ"))
  ])
)

NetworkAsset(
  name("DMZ_Network"),
  connectedThrough("Ethernet"),
  description("A network zone facilitating external communication through secure channels, including VPN servers and firewalls."),
  associatedHardware([
    HardwareAsset(name("Firewall_DMZ")),
    HardwareAsset(name("VPN_Server"))
  ])
)

NetworkAsset(
  name("Core_Data_Center_Network"),
  connectedThrough("Ethernet"),
  description("The central network connecting the data center and all critical servers, including RIS, DIS, LTO and PACS systems."),
  associatedHardware([
    HardwareAsset(name("Core_Switch")),
    HardwareAsset(name("Main_Server_PAGNI"))
  ])
```

```
)
```

```
Process(
  name("Medical_Imaging_Workflow"),
  description("The process involves capturing, storing, and retrieving medical imaging data, such as MRIs, CT
scans, and X-rays, for diagnostic purposes."),
  dependsOn("3"),  // Relies on PACS Server, RIS Server, and network assets
  involves([
    Asset(name("PACS_Server")),
    Asset(name("RIS_Server")),
    NetworkAsset(name("ICU_VLAN_20"))
  ])
)

Process(
  name("Laboratory_Data_Processing"),
  description("A process for handling laboratory data, including test sample collection, analysis, and result
reporting."),
  dependsOn("2"),  // Relies on Laboratory Information System and Administrative Network VLAN
  involves([
    Asset(name("Laboratory_Information_System")),
    NetworkAsset(name("Administrative_Network_VLAN_70"))
  ])
)

Process(
  name("Patient_Admission_and_Records_Management"),
  description("The workflow for admitting patients, creating electronic health records, and storing their
medical histories."),
  dependsOn("3"),  // Relies on Patient Records Database, Administrative Network, and VLAN 70
  involves([
    DataAsset(name("Patient_Records_Database")),
    NetworkAsset(name("Administrative_Network_VLAN_70")),
    HardwareAsset(name("ICT_Department_Server"))
  ])
)

Process(
  name("External_Communication_through_DMZ"),
  description("A secure communication workflow for interacting with external entities, such as remote
patients and partner organizations, through the DMZ Zone."),
  dependsOn("2"),  // Relies on VPN Server and Firewall_DMZ
  involves([
    HardwareAsset(name("VPN_Server")),
    HardwareAsset(name("Firewall_DMZ")),
    NetworkAsset(name("DMZ_Network"))
  ])
)
```

```
SecurityControl(
  name("Role-Based_Access_Control"),
  controlType("Software"),
  description("A software control restricting system access based on user roles, ensuring that only authorized
personnel can access sensitive data."),
  protects([
    DataAsset(name("Patient_Records_Database")),
    Asset(name("PACS_Server"))
  ]),
  addresses([
    SecurityProperty(name("Confidentiality")),
    SecurityProperty(name("Integrity"))
  ])
)

SecurityControl(
  name("Physical_Access_Control"),
  controlType("Physical"),
  description("A physical security measure restricting access to the data center, ensuring that only authorized
personnel can enter."),
  protects([
    HardwareAsset(name("Data_Center")),
    HardwareAsset(name("PACS_Server"))
  ]),
  addresses([
    SecurityProperty(name("Availability")),
    SecurityProperty(name("Confidentiality"))
  ])
)

SecurityControl(
  name("AES-256_Encryption"),
  controlType("Software"),
  description("A software-based encryption mechanism to secure sensitive data stored in the Patient Records
Database."),
  protects([
    DataAsset(name("Patient_Records_Database")),
    DataAsset(name("Lab_Test_Results_Data"))
  ]),
  addresses([
    SecurityProperty(name("Confidentiality"))
  ])
)

SecurityControl(
  name("Firewall_Protection"),
  controlType("Hardware"),
  description("A hardware firewall deployed in the DMZ zone to filter and block unauthorized traffic."),
  protects([
    NetworkAsset(name("DMZ_Network")),
    HardwareAsset(name("Firewall_DMZ"))
  ]),
  addresses([
    SecurityProperty(name("Availability")),
    SecurityProperty(name("Integrity"))
  ])
)

SecurityControl(
  name("Multi_Factor_Authentication"),
  controlType("Security Process"),
  description("A security process requiring users to verify their identity using multiple factors before accessing the administrative systems."),
  protects([
    DataAsset(name("Administrative_Records")),
    Asset(name("ICT_Department_Server"))
  ]),
  addresses([
    SecurityProperty(name("Confidentiality")),
    SecurityProperty(name("Integrity"))
  ])
)
```

```
SecurityProperty(
  name("Confidentiality_of_Patient_Records"),
  category("Confidentiality"),
  verification("Monitoring"),
  specification("Patient data must be encrypted using AES-256 and accessible only via Role-Based Access Control (RBAC)."),
  requiredOf([
    DataAsset(name("Patient_Records_Database")),
    Asset(name("PACS_Server"))
  ])
)

SecurityProperty(
  name("Availability_of_Medical_Imaging_Systems"),
  category("Availability"),
  verification("Testing"),
  specification("The PACS and RIS systems must be available 24/7 with a maximum downtime of 5 minutes per month."),
  requiredOf([
    Asset(name("PACS_Server")),
    Asset(name("RIS_Server"))
  ])
)

SecurityProperty(
  name("Integrity_of_Laboratory_Data"),
  category("Integrity"),
  verification("Static Analysis"),
  specification("Laboratory data must be validated against predefined standards to ensure accuracy and consistency."),
  requiredOf([
    DataAsset(name("Lab_Test_Results_Data")),
    Asset(name("Laboratory_Information_System"))
  ])
)

SecurityProperty(
  name("Privacy_of_Administrative_Records"),
  category("Privacy"),
  verification("Inspection"),
  specification("Administrative records must adhere to GDPR guidelines, ensuring that sensitive information
is anonymized when shared externally."),
  requiredOf([
    DataAsset(name("Administrative_Records")),
    Asset(name("ICT_Department_Server"))
  ])
)
```

5.1.3 Cyber Range Simulation and Training (CRST) Models - Training Programmes

5.1.3.1 Scenario 1: Identity Spoofing and Unauthorized Access via Phishing Emails

The CRST Model and its sub-models for the first scenario of Pilot 1, specified using the defined language, are presented below:

```
TrainingProgramme(
  name("Phishing_Emails_Training"),
  description("A structured training programme designed to equip personnel with the skills to identify,
report, and mitigate phishing attempts and prevent unauthorized access to sensitive systems."),
  goal("Identify and report at least 80% of phishing attempts and prevent unauthorized access."),
  role(["Administrative Staff", "IT Personnel"]),
  type("Detection and Response"),
  legalFramework("General Data Protection Regulation (GDPR), NIS Directive"),
  difficulty("3"),  // Medium difficulty
  covers([
    Asset(name("PACS_Server")),
    DataAsset(name("Patient_Records_Database"))
  ]),
  covers([
    Threat(name("Phishing_Attack"))
  ]),
  covers([
    SecurityProperty(name("Confidentiality_of_Patient_Records"))
  ]),
  covers([
    SecurityControl(name("Role-Based_Access_Control")),
    SecurityControl(name("AES-256_Encryption"))
  ]),
  records([
    Trace(
      name("Phishing_Trace"),
      description("A detailed log of participant activities during the training, including email analysis,
identification of phishing characteristics, and actions taken."),
      steps([
        "Trainee receives a simulated phishing email.",
        "Trainee identifies the phishing indicators (e.g., suspicious links, sender spoofing).",
        "Trainee reports the phishing email to IT security."
      ]),
      feedback([
        "Correct identification of phishing characteristics.",
        "Missed phishing indicators (e.g., urgency tone in email)."
      ]),
      outcomes([
        "Reported email flagged as phishing.",
        "Unauthorized access attempt prevented."
      ])
      )
   ]),
   supports([
      TrainingProgrammeExecution(
         name("Phishing_Programme_Execution"),
         accountRole(["IT Security Specialist", "Administrator"]),
         followedBy([
            Account(name("IT_Security_Account")),
            Account(name("Admin_Account"))
         ]),
         utilizedBy([
            Person(name("xxxxxx"), surname("xxxxxx")),
            Person(name("xxxxxx"), surname("xxxxxx"))
         ])
      )
   ]),
   consistsOf([
      Phase(
         name("Phishing_Email_Detection"),
         orderOfExecution("1"),
         isBasedOn(EventSequence(name("Phishing_Attack"))
      ),
      Phase(
         name("Incident_Response"),
         orderOfExecution("2"),
         isBasedOn(EventSequence(name("Unauthorized_Access_Attempt"))
      )
   ]),
   contains([
      SimulationModel(name("Phishing_Email_Simulation"))
   ]),
   includes([
      EmulationModel(name("Phishing_Email_Emulation"))
   ])
)
```

```
Simulation(
   name("Phishing_Email_Simulation"),
   description("A simulation model designed to replicate the behavior of an email server and the interaction of various network and user components to simulate phishing attacks and response strategies."),
   deploymentMode("pre-set"),
   tool("OMNeT++"),
   executionSpeed("x1.5"),
   randomSeed("12345"),
   message([
      "Simulated phishing email sent",
      "Response logged by email server",
      "Phishing detection triggered"
   ]),
   initialization("Initialize simulation environment with OMNeT++ configuration files"),
   isPartOf(TrainingProgramme(name("Phishing_Emails_Training"))),
   has([
      Phase(
         name("Phishing_Email_Simulation_Phase"),
         orderOfExecution("1"),
      isBasedOn(EventSequence(name("Phishing_Attack"))
    )
  ]),
  simulates([
    Asset(name("Email_Server")),
    NetworkAsset(name("Administrative_Network_VLAN_70"))
  ]),
  consistsOf([
    CompoundModule(
      name("Email_Server_Module"),
      parameters([
        "maxConnections: 100",
        "encryption: TLS 1.2"
      ]),
      properties([
        "performanceMetrics: latency, throughput",
        "visualization: enabled"
      ]),
      consistsOf([
        SimpleModule(
          name("SMTP_Handler"),
          handles([
            "Simulated phishing email",
            "Legitimate email"
          ])
        ),
        SimpleModule(
          name("Spam_Filter"),
          handles([
            "Email flagged as phishing",
            "Email marked as safe"
          ])
        )
      ])
    ),
    CompoundModule(
      name("Network_Switch_Module"),
      parameters([
        "bandwidth: 1Gbps",
        "latency: 5ms"
      ]),
      properties([
        "performanceMetrics: data rate, packet loss",
        "visualization: disabled"
      ]),
      consistsOf([
        SimpleModule(
          name("Packet_Processor"),
          handles([
            "Incoming data packets",
            "Outgoing data packets"
          ])
        )
      ])
    )
  ]),
  supports([
    Connection(
      name("Email_Server_to_Switch"),
      parameters([
        "protocol: SMTP",
        "encryption: TLS"
      ]),
      properties([
        "delay: 2ms",
        "datarate: 500Mbps"
      ]),
      behaviour("Bidirectional communication"),
      isPartOf(CRSTSimulationModel(name("Phishing_Email_Simulation")))
    )
  ])
)
```

```
Emulation(
  name("Phishing_Email_Emulation"),
  description("An emulation model designed to replicate the email server and its interactions with virtual and external components, enabling high-fidelity training in phishing detection and response."),
  deploymentMode("pre-set"),
  tool("OpenStack"),
  initialization("Instantiate and configure email server and network adapters using OpenStack."),
  isPartOf(TrainingProgramme(name("Phishing_Emails_Training"))),
  has([
    Phase(
      name("Phishing_Email_Emulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Phishing_Attack"))
    )
  ]),
  emulates([
    SoftwareAsset(name("Email_Server")),
    SoftwareAsset(name("Spam_Filter"))
  ]),
  involves([
    SoftwareAsset(name("SMTP_Service")),
    SoftwareAsset(name("Spam_Filter_Service"))
  ]),
  supports([
    VirtualNetworkModule(
      name("Email_Network_Connection"),
      connectionAsset([
        VirtualNetworkAdapter(
          IpInfo("Static", "192.168.1.10", "255.255.255.0"),
          MAC("02:42:ac:11:00:02"),
          Routing("Default Gateway: 192.168.1.1"),
          NetPort("Port 25", "TCP", "Open")
        ),
        VirtualNetworkAdapter(
          IpInfo("Static", "192.168.1.11", "255.255.255.0"),
          MAC("02:42:ac:11:00:03"),
          Routing("Default Gateway: 192.168.1.1"),
          NetPort("Port 443", "TCP", "Open")
```

```
            )
         ])
      )
   ])
)
```

5.1.3.2 Scenario 2: Incident Response - Detecting Unauthorized Access to PACS Storage

The CRST Model and its sub-models for the second scenario of Pilot 1, specified using the defined language, are presented below:

```
TrainingProgramme(
   name("Incident_Response_PACS_Access"),
   description("A structured training program designed to train IT and administrative personnel on detecting
unauthorized access to PACS storage, analyzing log files, and mitigating potential threats."),
   goal("Enable personnel to detect and respond to unauthorized access within 5 minutes of occurrence."),
   role(["IT Staff", "System Administrators"]),
   type("Incident Detection and Response"),
   legalFramework("HIPAA, GDPR"),
   difficulty("4"),  // Medium-high difficulty
   covers([
      Asset(name("PACS_Storage")),
      DataAsset(name("Medical_Images_Database"))
   ]),
   covers([
      Threat(name("Unauthorized_Access"))
   ]),
   covers([
      SecurityProperty(name("Integrity_of_Medical_Images")),
      SecurityProperty(name("Confidentiality_of_Medical_Data"))
   ]),
   covers([
      SecurityControl(name("Log_Analysis_Tool")),
      SecurityControl(name("Access_Control_Mechanism"))
   ]),
   records([
      Trace(
         name("PACS_Incident_Trace"),
         description("Detailed record of trainee activities during the training, including log analysis,
identification of unauthorized access patterns, and response actions."),
         steps([
            "Trainee accesses the PACS log management system.",
            "Trainee identifies anomalies in access logs.",
            "Trainee mitigates unauthorized access and secures the system."
         ]),
         feedback([
            "Correct identification of suspicious patterns.",
            "Effective response time within the set threshold."
         ]),
         outcomes([
            "Unauthorized access blocked.",
            "System integrity restored."
         ])
      )
   ]),
  supports([
    TrainingProgrammeExecution(
      name("PACS_Access_Response_Execution"),
      accountRole(["IT Specialist"]),
      followedBy([
        Account(name("IT_Account")),
        Account(name("Admin_Account"))
      ]),
      utilizedBy([
        Person(name("xxxxxx"), surname("xxxxxx")),
        Person(name("xxxxxx"), surname("xxxxxx"))
      ])
    )
  ]),
  consistsOf([
    Phase(
      name("Log_Analysis"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Unauthorized_Access_Detection"))
    ),
    Phase(
      name("System_Secure"),
      orderOfExecution("2"),
      isBasedOn(EventSequence(name("Access_Control_Implementation"))
    )
  ]),
  contains([
    SimulationModel(name("PACS_Log_Analysis_Simulation"))
  ]),
  includes([
    EmulationModel(name("PACS_Server_Emulation"))
  ])
)
```

```
Simulation(
  name("PACS_Log_Analysis_Simulation"),
  description("A simulation model designed to mimic PACS storage behavior and log access events, including
unauthorized attempts."),
  deploymentMode("pre-set"),
  tool("OMNeT++"),
  executionSpeed("x1"),
  randomSeed("67890"),
  message([
    "Log access attempt recorded",
    "Unauthorized access detected",
    "Response action triggered"
  ]),
  initialization("Initialize PACS storage simulation environment using OMNeT++ configuration."),
  isPartOf(TrainingProgramme(name("Incident_Response_PACS_Access"))),
  has([
    Phase(
      name("Log_Analysis_Simulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Unauthorized_Access_Detection"))
    )
```

```
   ]),
   simulates([
      Asset(name("PACS_Storage")),
      DataAsset(name("Medical_Images_Database"))
   ]),
   consistsOf([
      CompoundModule(
         name("Log_Manager_Module"),
         parameters([
            "logRetention: 30 days",
            "anomalyThreshold: 90%"
         ]),
         properties([
            "performanceMetrics: detection rate, false positives",
            "visualization: enabled"
         ]),
         consistsOf([
            SimpleModule(
               name("Log_Processor"),
               handles([
                  "Access logs",
                  "Anomaly detection alerts"
               ])
            ),
            SimpleModule(
               name("Alert_Manager"),
               handles([
                  "Unauthorized access alerts",
                  "Notification events"
               ])
            )
         ])
      )
   ])
)
```

```
Emulation(
   name("PACS_Server_Emulation"),
   description("An emulation model replicating the PACS server's functionality, enabling trainees to interact with real-world data access scenarios."),
   deploymentMode("pre-set"),
   tool("OpenStack"),
   initialization("Instantiate and configure PACS server and virtual adapters using OpenStack."),
   isPartOf(TrainingProgramme(name("Incident_Response_PACS_Access"))),
   has([
      Phase(
         name("PACS_Emulation_Phase"),
         orderOfExecution("1"),
         isBasedOn(EventSequence(name("Unauthorized_Access_Attempt"))
      )
   ]),
   emulates([
      SoftwareAsset(name("PACS_Server")),
      DataAsset(name("Medical_Images_Database"))
   ]),
   involves([
      SoftwareAsset(name("Access_Logger")),
      SoftwareAsset(name("Alert_System"))
   ]),
   supports([
      VirtualNetworkModule(
         name("PACS_Network_Connection"),
         connectionAsset([
            VirtualNetworkAdapter(
               IpInfo("Static", "192.168.2.10", "255.255.255.0"),
               MAC("02:42:ac:11:00:04"),
               Routing("Default Gateway: 192.168.2.1"),
               NetPort("Port 443", "TCP", "Open")
            )
         ])
      )
   ])
)
```

5.1.3.3 Scenario 3: Denial of Service Attack on Hospital Systems

The CRST Model and its sub-models for the third scenario of Pilot 1, specified using the defined language, are presented below:

```
TrainingProgramme(
   name("DoS_Attack_Mitigation_Training"),
   description("A structured training program designed to equip IT staff and system administrators with the
skills to detect, mitigate, and respond to Denial of Service (DoS) attacks targeting critical hospital systems."),
   goal("Train personnel to identify and mitigate DoS attacks within 10 minutes of detection."),
   role(["IT Staff", "System Administrators"]),
   type("Detection and Response"),
   legalFramework("GDPR, NIS Directive"),
   difficulty("5"),  // High difficulty
   covers([
      Asset(name("Hospital_Network")),
      NetworkAsset(name("VLAN_70"))
   ]),
   covers([
      Threat(name("DoS_Attack"))
   ]),
   covers([
      SecurityProperty(name("Availability_of_Hospital_Systems"))
   ]),
   covers([
      SecurityControl(name("Network_Traffic_Filtering")),
      SecurityControl(name("Firewall_Rule_Set"))
   ]),
   records([
      Trace(
         name("DoS_Trace"),
         description("Detailed record of trainee activities, including traffic analysis, attack mitigation, and post-
event actions."),
         steps([
            "Trainee accesses network monitoring tools.",
            "Trainee identifies unusual traffic patterns.",
        "Trainee applies filtering rules to block malicious traffic."
      ]),
      feedback([
        "Correct identification of attack vectors.",
        "Timely application of mitigation measures."
      ]),
      outcomes([
        "Traffic normalized.",
        "Systems restored to operational state."
      ])
    )
  ]),
  supports([
    TrainingProgrammeExecution(
      name("DoS_Attack_Response_Execution"),
      accountRole(["IT Specialist", "Network Engineer"]),
      followedBy([
        Account(name("IT_Security_Account")),
        Account(name("Network_Admin_Account"))
      ]),
      utilizedBy([
        Person(name("xxxxxx"), surname("xxxxxx")),
        Person(name("xxxxxx"), surname("xxxxxx"))
      ])
    )
  ]),
  consistsOf([
    Phase(
      name("Traffic_Analysis"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("DoS_Attack_Detection"))
    ),
    Phase(
      name("Mitigation"),
      orderOfExecution("2"),
      isBasedOn(EventSequence(name("Traffic_Blocking"))
    )
  ]),
  contains([
    SimulationModel(name("DoS_Traffic_Simulation"))
  ]),
  includes([
    EmulationModel(name("Hospital_Network_Emulation"))
  ])
)
```

```
Simulation(
  name("DoS_Traffic_Simulation"),
  description("A simulation model designed to replicate network behavior during a DoS attack, including
abnormal traffic patterns and system resource exhaustion."),
  deploymentMode("pre-set"),
  tool("OMNeT++"),
  executionSpeed("x2"),
  randomSeed("24680"),
  message([
     "High traffic volume detected",
     "Service unresponsive",
     "Mitigation measures applied"
  ]),
  initialization("Initialize network simulation environment with DoS traffic generation."),
  isPartOf(TrainingProgramme(name("DoS_Attack_Mitigation_Training"))),
  has([
     Phase(
        name("Traffic_Analysis_Phase"),
        orderOfExecution("1"),
        isBasedOn(EventSequence(name("DoS_Attack_Detection"))
     )
  ]),
  simulates([
     NetworkAsset(name("Hospital_Network")),
     Asset(name("Firewall"))
  ]),
  consistsOf([
     CompoundModule(
        name("Traffic_Generator_Module"),
        parameters([
           "attackTrafficRate: 10Gbps",
           "attackDuration: 5 minutes"
        ]),
        properties([
           "performanceMetrics: packet drop rate, latency",
           "visualization: enabled"
        ]),
        consistsOf([
           SimpleModule(
              name("Traffic_Analyzer"),
              handles([
                 "Incoming attack packets",
                 "Normal traffic packets"
              ])
           ),
           SimpleModule(
              name("Mitigation_Handler"),
              handles([
                 "Traffic filtering rules",
                 "Blocked IP addresses"
              ])
           )
        ])
     )
  ])
)
```

```
Emulation(
   name("Hospital_Network_Emulation"),
   description("An emulation model replicating the hospital's network infrastructure, enabling trainees to respond to a simulated DoS attack in real-time."),
   deploymentMode("pre-set"),
   tool("OpenStack"),
   initialization("Instantiate and configure hospital network and firewalls using OpenStack."),
  isPartOf(TrainingProgramme(name("DoS_Attack_Mitigation_Training"))),
  has([
    Phase(
      name("Network_Emulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("DoS_Attack_Execution"))
    )
  ]),
  emulates([
    NetworkAsset(name("Hospital_Network")),
    NetworkAsset(name("VLAN_70"))
  ]),
  involves([
    HardwareAsset(name("Firewall")),
    SoftwareAsset(name("Traffic_Monitoring_Tool"))
  ]),
  supports([
    VirtualNetworkModule(
      name("DoS_Network_Connection"),
      connectionAsset([
        VirtualNetworkAdapter(
          IpInfo("Dynamic", "192.168.3.20", "255.255.255.0"),
          MAC("02:42:ac:11:00:05"),
          Routing("Default Gateway: 192.168.3.1"),
          NetPort("Port 80", "TCP", "Open")
        ),
        VirtualNetworkAdapter(
          IpInfo("Dynamic", "192.168.3.21", "255.255.255.0"),
          MAC("02:42:ac:11:00:06"),
          Routing("Default Gateway: 192.168.3.1"),
          NetPort("Port 443", "TCP", "Open")
        )
      ])
    )
  ])
)
```

5.2 Pilot 2: Healthcare Authority (PAGNI)

5.2.1 Overview

This section focuses on the CRSA and the CRST models developed for the Healthcare Authority pilot at PAGNI. The continuous monitoring and adaptation capabilities of the AERAS platform ensure that the training outcomes contribute directly to improving PAGNI’s overall security posture, providing actionable insights into the effectiveness of the cybersecurity measures implemented. Same as with the first pilot above, the names and personal information presented are entirely artificial.

5.2.2 Cyber Range Security Assurance (CRSA) Models

The CRSA Model and its sub-models for the first pilot, specified using the defined language, are presented below:

```
SecurityAssurance(
  name("PAGNI_CyberSecurity_Assurance_Model"),
    dateFrom("2024-09-23"),
    dateTo(null),
    description("The primary security assurance model for the PAGNI pilot, outlining the core structure for
addressing cybersecurity challenges across its infrastructure."),
    creator(
        Person(
            name("Dimitris"),
            surname("Alexiou"),
            organisation("University of Patras"),
            role(system_administrator)
        )
    )
)
```

```
Vulnerability(
    name("Outdated_VPN_Server_Software"),
    source("National Vulnerability Database (NVD)"),
    publishedDate("2024-09-23"),
    lastModified("2024-09-23"),
    vulnerabilityType("Computational"),
    description("The VPN server software is running an older version with known vulnerabilities, allowing
attackers to bypass authentication and gain unauthorized access."),
    mitigatedBy(SecurityControl(name("Regular_Software_Updates"))),
    appliesTo(Asset(name("VPN_Server"), assetType("Software"))),
    canBeExploitedBy(Violation(name("Unauthorized_Network_Access"))),
    couldLeadToViolationOf(SecurityProperty(name("Confidentiality")))
)

Vulnerability(
    name("Unsecured_WiFi_Networks"),
    source("Internal Security Assessment Report"),
    publishedDate("2024-09-23"),
    lastModified("2024-09-23"),
    vulnerabilityType("Physical"),
    description("Wi-Fi networks in Buildings A, B, and C lack adequate encryption and authentication
mechanisms, leaving them susceptible to man-in-the-middle (MITM) attacks."),
    mitigatedBy(SecurityControl(name("WPA3_Encryption"))),
    appliesTo(Asset(name("WiFi_Routers"), assetType("Hardware"))),
    canBeExploitedBy(Violation(name("Eavesdropping"))),
    couldLeadToViolationOf(SecurityProperty(name("Integrity")))
)

Vulnerability(
    name("Misconfigured_Firewall_Rules"),
    source("PAGNI IT Department Audit"),
    publishedDate("2024-09-23"),
    lastModified("2024-09-23"),
    vulnerabilityType("Computational"),
    description("The firewall in the DMZ zone is misconfigured, allowing excessive open ports and unauthorized
inbound traffic."),
    mitigatedBy(SecurityControl(name("Firewall_Configuration_Review"))),
    appliesTo(Asset(name("Firewall"), assetType("Hardware"))),
    canBeExploitedBy(Violation(name("Unauthorized_Traffic_Flow"))),
    couldLeadToViolationOf(SecurityProperty(name("Availability")))
)
```

```
Vulnerability(
    name("Lack_of_MFA_for_HIS"),
    source("External Security Audit"),
    publishedDate("2024-09-23"),
    lastModified("2024-09-23"),
    vulnerabilityType("Computational"),
    description("The Hospital Information System (HIS) lacks multi-factor authentication, making it vulnerable to credential theft and unauthorized access."),
    mitigatedBy(SecurityControl(name("MFA_Implementation"))),
    appliesTo(Asset(name("HIS"), assetType("Software"))),
    canBeExploitedBy(Violation(name("Credential_Theft"))),
    couldLeadToViolationOf(SecurityProperty(name("Confidentiality")))
)
```

```
Threat(
    name("Phishing_Attack"),
    likelihood("High"),
    source("ENISA Threat Landscape Report 2024"),
    category("Social Engineering"),
    description("A phishing attack targeting hospital administrative staff and IT personnel to steal credentials and gain unauthorized access to sensitive systems like HIS and LIS."),
    mayViolate(SecurityProperty(name("Confidentiality"))),
    mayViolate(SecurityProperty(name("Integrity")))
)

Threat(
    name("Impersonation_Attempt"),
    likelihood("High"),
    source("ENISA Threat Landscape Report 2024"),
    category("Social Engineering"),
    description("An impersonation attempt targeting hospital administrative staff and IT personnel to steal credentials and gain unauthorized access to sensitive systems like HIS and LIS."),
    mayViolate(SecurityProperty(name("Confidentiality"))),
    mayViolate(SecurityProperty(name("Integrity")))
)

Threat(
    name("Ransomware_Attack"),
    likelihood("Medium"),
    source("Internal Security Incident Report 2023"),
    category("Malware"),
    description("A ransomware attack aiming to encrypt critical hospital systems, including PACS, HIS, and LIS, causing disruption in patient care and data access."),
    mayViolate(SecurityProperty(name("Availability"))),
    mayViolate(SecurityProperty(name("Confidentiality"))),
    mayViolate(SecurityProperty(name("Integrity")))
)

Threat(
    name("Misconfigured_System_Exploitation"),
    likelihood("Medium"),
    source("PAGNI IT Department Assessment"),
    category("Configuration"),
    description("Exploitation of misconfigured systems, such as firewalls or routers, leading to unauthorized
access, traffic rerouting, or service disruptions."),
    mayViolate(SecurityProperty(name("Availability"))),
    mayViolate(SecurityProperty(name("Confidentiality"))),
    mayViolate(SecurityProperty(name("Integrity")))
)
```

```
Asset(
  name("PAGNI_Data_Center"),
  owner(Person(name("Eleni"), surname("Karamanou"), role("System Administrator"))),
  value("€200,000"),
  description("The primary data center housing critical hospital systems such as HIS, LIS, and PACS."),
  protectedBy(SecurityControl(name("Access_Control_Policies"))),
  contains(Asset(name("PAGNI_Main_Server"))),
  communicatesThrough(NetworkAsset(name("VLAN_90")))
)

Asset(
  name("DMZ_Zone"),
  owner(Person(name("Vasilis"), surname("Georgiou"), role("IT Security Specialist"))),
  value("€30,000"),
  description("A demilitarized zone managing external connections and traffic flow through firewalls, VPN
servers, and security servers."),
  protectedBy(SecurityControl(name("Firewall_Rule_Set"))),
  contains(Asset(name("VPN_Server"))),
  communicatesThrough(NetworkAsset(name("VLAN_80")))
)

Asset(
  name("PAGNI_Main_Server"),
  vendor("Dell"),
  version("PowerEdge R740"),
  managedBy(Person(name("Christos"), surname("Papadakis"), role("Network Engineer"))),
  operatesIn(Asset(name("PAGNI_Data_Center"))),
  value("€50,000"),
  description("Central server hosting the PACS, HIS, and LIS applications essential for hospital operations."),
  protectedBy(SecurityControl(name("Endpoint_Protection_Suite"))),
  communicatesThrough(NetworkAsset(name("VLAN_90")))
)

Asset(
  name("DMZ_Firewall"),
  vendor("Cisco"),
  version("ASA 5500-X"),
  managedBy(Person(name("Vasilis"), surname("Georgiou"), role("IT Security Specialist"))),
  operatesIn(Asset(name("DMZ_Zone"))),
  value("€10,000"),
  description("Firewall protecting internal networks from unauthorized external traffic."),
  protectedBy(SecurityControl(name("Firewall_Rule_Set"))),
  communicatesThrough(NetworkAsset(name("VLAN_80")))
)

Asset(
  name("WiFi_Router_Building_A"),
  vendor("Aruba"),
  version("303 Series"),
  managedBy(Person(name("Maria"), surname("Nikolaou"), role("Network Technician"))),
  operatesIn(Asset(name("Building_A"))),
  value("€1,200"),
  description("Wireless router providing internet and internal network connectivity for Building A."),
  protectedBy(SecurityControl(name("WPA3_Encryption"))),
  communicatesThrough(NetworkAsset(name("VLAN_30")))
)

Asset(
  name("Building_A_Network_Cabling"),
  physicalType("RJ-45 Ethernet Cables"),
  owner(Person(name("Maria"), surname("Nikolaou"), role("Network Technician"))),
  value("€5,000"),
  description("Physical cabling connecting the network devices within Building A's clinic."),
  isContainedIn(Asset(name("Building_A"))),
  protectedBy(SecurityControl(name("Physical_Access_Locks")))
)

Asset(
  name("Radiology_Network_Cabling"),
  physicalType("Fiber Optic"),
  owner(Person(name("Ioanna"), surname("Markou"), role("Radiology IT Specialist"))),
  value("€8,000"),
  description("Fiber optic cables connecting imaging devices to PACS for data transfer."),
  isContainedIn(Asset(name("Building_D"))),
  protectedBy(SecurityControl(name("Access_Control_Policies")))
)
```

```
SoftwareAsset(
  name("HIS"),
  level("SAL"),
  description("The Hospital Information System is responsible for managing patient records, appointments,
and administrative data."),
  provides(Interface(name("Patient_Record_API"), description("API for managing patient data"))),
  requires(Interface(name("LIS_API"), description("Interface for accessing laboratory results"))),
  providesImplTo(InterfaceImp(
    impType("REST"),
    accessEndPoint("https://his.pagni.gr/api"),
    codeFile("his_api_v1.0.zip")
  ))
)

SoftwareAsset(
  name("PACS_ Server"),
  level("SAL"),
  description("System for storing, retrieving, and distributing medical imaging data for radiology and other
departments."),
  provides(Interface(name("Imaging_Data_API"), description("API for accessing medical imaging data"))),
  requires(Interface(name("HIS_API"), description("Interface for accessing patient records"))),
  providesImplTo(InterfaceImp(
    impType("SOAP"),
    accessEndPoint("https://pacs.pagni.gr/api"),
    codeFile("pacs_api_v2.3.zip")
  ))
)

SoftwareAsset(
   name("LIS"),
   level("SAL"),
   description("The Laboratory Information System manages laboratory test results and their integration with
other hospital systems."),
   provides(Interface(name("Lab_Results_API"), description("API for accessing laboratory test results"))),
   requires(Interface(name("HIS_API"), description("Interface for patient demographic data"))),
   providesImplTo(InterfaceImp(
      impType("REST"),
      accessEndPoint("https://lis.pagni.gr/api"),
      codeFile("lis_api_v3.1.zip")
   ))
)

Interface(
   name("Patient_Record_API"),
   description("API for managing patient data"),
   isProvidedBy(SoftwareAsset(name("HIS"))),
   isRequiredBy(SoftwareAsset(name("PACS")))
)

InterfaceImp(
   name("REST_Implementation"),
   impType("REST"),
   accessEndPoint("https://his.pagni.gr/api"),
   codeFile("his_api_v1.0.zip"),
   implements(Interface(name("Patient_Record_API")))
)
```

```
HardwareAsset(
   name("Main_Server_PAGNI"),
   hwType("Computational"),
   description("Primary server hosting HIS, LIS, and PACS applications for the hospital."),
   hasSubmodule(MemoryModule(
      noOfModules("4"),
      memorySize("32GB"),
      memoryType("DDR5"),
      memorySpeed("3200 MHz"),
      memoryManufacturer("Kingston")
   )),
   hasSubmodule(DriveModule(
      driveLocation("RAID Array"),
      noOfDrives("6"),
      driveController("SAS"),
      driveFirmware("v1.5.2"),
      driveCapacity("2TB each")
   )),
   hasSubmodule(CPUModule(
      processorName("Intel Xeon Gold 6226R"),
      numberOfCores("16"),
      numberOfThreads("32"),
      processorBaseFrequency("2.9 GHz"),
      socket("LGA3647")
```

```
  )),
  isPartOf(HardwareAsset(name("PAGNI_Data_Center")))
)

HardwareAsset(
  name("DMZ_Router"),
  hwType("Network"),
  description("Router facilitating secure communication between internal systems and external services."),
  hasSubmodule(PortModule(
    ioPort("Ethernet"),
    isAlwaysConnected("True")
  )),
  isPartOf(HardwareAsset(name("DMZ_Zone")))
)

HardwareAsset(
  name("WiFi_Router_Building_A"),
  hwType("Network"),
  description("Wireless router providing network connectivity for Building A clinic."),
  hasSubmodule(PortModule(
    ioPort("Ethernet"),
    isAlwaysConnected("False")
  )),
  isPartOf(HardwareAsset(name("Building_A")))
)

HardwareAsset(
  name("Memory_Module_Server"),
  hwType("Memory"),
  description("Memory module for the main server in the PAGNI Data Center."),
  noOfModules("4"),
  memorySize("32GB"),
  memoryType("DDR5"),
  memorySpeed("3200 MHz"),
  memoryManufacturer("Kingston")
)

HardwareAsset(
  name("Radiology_Workstation"),
  hwType("Medical Workstation"),
  description("High-performance workstation for processing and analyzing medical imaging data."),
  hasSubmodule(CPUModule(
    processorName("Intel Core i9-12900K"),
    numberOfCores("16"),
    numberOfThreads("24"),
    processorBaseFrequency("3.2 GHz"),
    socket("LGA1700")
  )),
  hasSubmodule(MemoryModule(
    noOfModules("2"),
    memorySize("64GB"),
    memoryType("DDR5"),
    memorySpeed("4800 MHz"),
    memoryManufacturer("Corsair")
  )),
  isPartOf(HardwareAsset(name("Building_D_Radiology_Department")))
```

```
)

HardwareAsset(
   name("Drive_Module_Server"),
   hwType("Drive"),
   description("Storage drives for the main server in the PAGNI Data Center."),
   driveLocation("RAID Array"),
   noOfDrives("6"),
   driveController("SAS"),
   driveFirmware("v1.5.2"),
   driveCapacity("2TB each")
)

HardwareAsset(
   name("CPU_Module_Server"),
   hwType("Processor"),
   description("Central Processing Unit for the main server."),
   processorName("Intel Xeon Gold 6226R"),
   numberOfCores("16"),
   numberOfThreads("32"),
   ProcessorBaseFrequency("2.9 GHz"),
   Socket("LGA3647")
)
```

```
DataAsset(
   name("Patient_Records_Database"),
   dataType("Operational"),
   dataState("At_Rest"),
   description("A central repository containing sensitive patient health records, including diagnostic results,
medical histories, and treatment plans."),
   storageLocation(Asset(name("HIS_Server"))),
   accessControls(SecurityControl(name("Role-Based Access Control"))),
   encryptionStatus("Enabled (AES-256)"),
   classification("Confidential")
)

DataAsset(
   name("Lab_Test_Results_Data"),
   dataType("Operational"),
   dataState("In_Processing"),
   description("Laboratory test results, such as blood work and chemical analysis, processed and managed by
the LIS."),
   storageLocation(Asset(name("Laboratory_Information_System"))),
   accessControls(SecurityControl(name("Access Control List (ACL)"))),
   encryptionStatus("Enabled (SSL/TLS)"),
   classification("Sensitive")
)

DataAsset(
   name("Medical_Imaging_Data"),
   dataType("Operational"),
   dataState("At_Rest"),
   description("Medical imaging data such as MRI, CT scans, and X-rays stored within the PACS."),
   storageLocation(Asset(name("PACS_Server"))),
   accessControls(SecurityControl(name("Multi-Factor Authentication"))),
   encryptionStatus("Enabled (AES-256)"),
   classification("Confidential")
)

DataAsset(
   name("IT_Infrastructure_Logs"),
   dataType("Configuration"),
   dataState("At_Rest"),
   description("System logs detailing activities, configurations, and events for auditing and troubleshooting."),
   storageLocation(Asset(name("DMZ_Security_Server"))),
   accessControls(SecurityControl(name("Encrypted File Access"))),
   encryptionStatus("Enabled (AES-128)"),
   classification("Restricted")
)

DataAsset(
   name("Administrative_Records"),
   dataType("Admin"),
   dataState("At_Rest"),
   description("Hospital administrative data including employee records, financial transactions, and resource allocations."),
   storageLocation(Asset(name("Administrative_Server"))),
   accessControls(SecurityControl(name("Role-Based Access Control"))),
   encryptionStatus("Enabled (SSL/TLS)"),
   classification("Confidential")
)

DataAsset(
   name("Network_Configuration_Data"),
   dataType("Configuration"),
   dataState("At_Rest"),
   description("Configuration files for network devices such as routers, switches, and firewalls."),
   storageLocation(Asset(name("IT_Department_Server"))),
   accessControls(SecurityControl(name("Access Control List (ACL)"))),
   encryptionStatus("Enabled (AES-128)"),
   classification("Restricted")
)
```

```
Person(
  name("Katerina"),
  surname("Papadaki"),
  dateOfBirth("YYYY-MM-DD"),
  role("Asset Owner"),
  description("Head of IT Security at PAGNI, responsible for overseeing the security of all computational and data assets within the organization."),
  associatedAssets([
    Asset(name("DMZ_Router")),
    Asset(name("Patient_Records_Database")),
    Asset(name("IT_Infrastructure_Logs"))
  ])
)

Person(
  name("Dimitris"),
  surname("Vasilakis"),
  dateOfBirth("YYYY-MM-DD"),
  role("Lab IT Specialist"),
  description("Responsible for managing and securing the Laboratory Information System (LIS) and associated
data assets."),
  associatedAssets([
    Asset(name("Laboratory_Information_System")),
    Asset(name("Lab_Test_Results_Data"))
  ])
)

Person(
  name("xxxxxx"),
  surname("xxxxxx"),
  dateOfBirth("YYYY-MM-DD"),
  role("Radiology IT Specialist"),
  description("Oversees the PACS system and ensures the security of medical imaging data."),
  associatedAssets([
    Asset(name("PACS_Server")),
    Asset(name("Medical_Imaging_Data"))
  ])
)

Person(
  name("xxxxxx"),
  surname("xxxxxx"),
  dateOfBirth("YYYY-MM-DD"),
  role("Network Engineer"),
  description("Maintains the hospital's network infrastructure, including routers, firewalls, and network
configuration files."),
  associatedAssets([
    Asset(name("DMZ_Router")),
    Asset(name("Network_Configuration_Data"))
  ])
)

Person(
  name("xxxxxx"),
  surname("xxxxxx"),
  dateOfBirth("YYYY-MM-DD"),
 role("Administrative Staff"),
  description("Handles administrative operations and ensures the proper management of hospital records
and resources."),
  associatedAssets([
    Asset(name("Administrative_Records"))
  ])
)
```

```
NetworkAsset(
  name("Clinics_VLAN_30"),
  connectedThrough("Ethernet"),
  description("A network segment dedicated to Building A clinics, ensuring secure communication and data
exchange within the building."),
  associatedHardware([
    HardwareAsset(name("Switch_Building_A")),
    HardwareAsset(name("WiFi_Router_Building_A"))
```

```
   ])
)

NetworkAsset(
   name("Clinics_VLAN_40"),
   connectedThrough("Ethernet"),
   description("A network segment dedicated to Building B clinics, ensuring reliable data connectivity for
healthcare systems."),
   associatedHardware([
      HardwareAsset(name("Switch_Building_B")),
      HardwareAsset(name("WiFi_Router_Building_B"))
   ])
)

NetworkAsset(
   name("Clinics_VLAN_50"),
   connectedThrough("Ethernet"),
   description("A network segment dedicated to Building C clinics, ensuring reliable data connectivity for
healthcare systems."),
   associatedHardware([
      HardwareAsset(name("Switch_Building_C")),
      HardwareAsset(name("WiFi_Router_Building_C"))
   ])
)

NetworkAsset(
   name("Radiology_VLAN_60_70"),
   connectedThrough("Ethernet"),
   description("A VLAN segment for the Radiology Department, facilitating secure data transmission for
imaging devices like MRI, CT, and X-Ray machines."),
   associatedHardware([
      HardwareAsset(name("Switch_Radiology")),
      HardwareAsset(name("PACS_Server"))
   ])
)

NetworkAsset(
   name("Laboratory_VLAN_80"),
   connectedThrough("Ethernet"),
   description("A VLAN segment for the Laboratory Department, ensuring secure communication for LIS and
other laboratory systems."),
   associatedHardware([
      HardwareAsset(name("Switch_Laboratory")),
      HardwareAsset(name("Laboratory_Information_System"))
   ])
)

NetworkAsset(
   name("IT_Department_VLAN_90"),
   connectedThrough("Ethernet"),
   description("A dedicated VLAN for the IT Department, supporting secure data exchange for IT systems and
administrative operations."),
   associatedHardware([
      HardwareAsset(name("Switch_IT_Department")),
      HardwareAsset(name("DMZ_Router"))
   ])
```

```
)

NetworkAsset(
  name("Administrative_VLAN_100"),
  connectedThrough("Ethernet"),
  description("A VLAN segment for the Administrative Department, handling sensitive administrative and financial data."),
  associatedHardware([
    HardwareAsset(name("Switch_Administrative")),
    HardwareAsset(name("Administrative_Server"))
  ])
)

NetworkAsset(
  name("DMZ_Network"),
  connectedThrough("Ethernet"),
  description("The DMZ network segment enabling secure communication between external systems and internal services."),
  associatedHardware([
    HardwareAsset(name("Firewall_DMZ")),
    HardwareAsset(name("VPN_Server")),
    HardwareAsset(name("Security_Server"))
  ])
)

NetworkAsset(
  name("Core_Data_Center_Network"),
  connectedThrough("Ethernet"),
  description("The central network connecting the data center and all critical servers, including HIS, LIS, and PACS systems."),
  associatedHardware([
    HardwareAsset(name("Core_Switch")),
    HardwareAsset(name("Main_Server_PAGNI"))
  ])
)
```

```
Process(
  name("Hospital_Admissions_Workflow"),
  description("The process of registering and admitting patients, capturing their personal and medical data, and assigning them to respective clinics or departments."),
  dependsOn("4"),  // Relies on HIS, Administrative Server, Patient Database, and Clinics VLAN
  involves([
    Asset(name("HIS_Server")),
    Asset(name("Administrative_Server")),
    DataAsset(name("Patient_Records_Database")),
    NetworkAsset(name("Clinics_VLAN_30"))
  ])
)

Process(
  name("Laboratory_Test_Results_Processing"),
  description("The process of collecting, analyzing, and storing laboratory test results, such as blood tests and virology data."),
  dependsOn("3"),  // Relies on LIS Server, Lab Test Database, and Laboratory VLAN
  involves([
        Asset(name("Laboratory_Information_System")),
        DataAsset(name("Lab_Test_Results_Data")),
        NetworkAsset(name("Laboratory_VLAN_80"))
    ])
)

Process(
    name("Radiology_Data_Management_Workflow"),
    description("The process of capturing, storing, and accessing radiology imaging data, such as CT scans,
MRIs, and X-rays, for diagnostic purposes."),
    dependsOn("3"),  // Relies on PACS Server, Imaging Equipment, and Radiology VLAN
    involves([
        Asset(name("PACS_Server")),
        HardwareAsset(name("MRI_Device")),
        NetworkAsset(name("Radiology_VLAN_60"))
    ])
)

Process(
    name("Administrative_Records_Management"),
    description("The process of managing administrative data, including financial records, staff information,
and hospital operations."),
    dependsOn("3"),  // Relies on Administrative Server, Records Database, and Administrative VLAN
    involves([
        Asset(name("Administrative_Server")),
        DataAsset(name("Administrative_Records")),
        NetworkAsset(name("Administrative_VLAN_100"))
    ])
)

Process(
    name("IT_Incident_Response_Workflow"),
    description("The process of detecting, analyzing, and responding to cybersecurity incidents, such as
unauthorized access or ransomware attacks."),
    dependsOn("4"),  // Relies on IT Logs, Security Server, DMZ Router, and IT VLAN
    involves([
        DataAsset(name("IT_Infrastructure_Logs")),
        HardwareAsset(name("Security_Server")),
        NetworkAsset(name("DMZ_Network")),
        NetworkAsset(name("IT_Department_VLAN_100"))
    ])
)

Process(
    name("Data_Backup_and_Recovery_Process"),
    description("The process of creating, storing, and recovering backups of critical hospital systems, such as
HIS, LIS, and PACS."),
    dependsOn("5"),  // Relies on Backup Server, Data Center Network, and individual system assets
    involves([
        Asset(name("Backup_Server")),
        NetworkAsset(name("Core_Data_Center_Network")),
        Asset(name("HIS_Server")),
        Asset(name("Laboratory_Information_System")),
        Asset(name("PACS_Server"))
    ])
)
```

```
SecurityControl(
   name("Role-Based_Access_Control"),
   controlType("Software"),
   description("Restricts access to specific hospital systems and data based on user roles, ensuring that only authorized personnel can perform certain actions."),
   protects([
      DataAsset(name("Patient_Records_Database")),
      DataAsset(name("Lab_Test_Results_Data")),
      Asset(name("HIS_Server"))
   ]),
   addresses([
      SecurityProperty(name("Confidentiality")),
      SecurityProperty(name("Integrity"))
   ])
)

SecurityControl(
   name("Network_Firewall_Protection"),
   controlType("Hardware"),
   description("A hardware firewall designed to monitor and control incoming and outgoing network traffic based on security rules."),
   protects([
      NetworkAsset(name("DMZ_Network")),
      NetworkAsset(name("IT_Department_VLAN_100")),
      NetworkAsset(name("Radiology_VLAN_60"))
   ]),
   addresses([
      SecurityProperty(name("Confidentiality")),
      SecurityProperty(name("Availability"))
   ])
)

SecurityControl(
   name("Multi-Factor_Authentication"),
   controlType("Software"),
   description("Adds an additional layer of authentication for users accessing critical hospital systems."),
   protects([
      Asset(name("HIS_Server")),
      Asset(name("Administrative_Server")),
      DataAsset(name("Administrative_Records"))
   ]),
   addresses([
      SecurityProperty(name("Integrity")),
      SecurityProperty(name("Confidentiality"))
   ])
)

SecurityControl(
   name("Antivirus_Malware_Protection"),
   controlType("Software"),
   description("Detects, prevents, and removes malware from critical systems to ensure operational integrity."),
   protects([
      Asset(name("Laboratory_Information_System")),
        Asset(name("PACS_Server")),
        HardwareAsset(name("Administrative_Server"))
    ]),
    addresses([
        SecurityProperty(name("Integrity")),
        SecurityProperty(name("Availability"))
    ])
)

SecurityControl(
    name("AES-256_Data_Encryption"),
    controlType("Software"),
    description("Encrypts sensitive data, such as patient records and laboratory results, to ensure data
confidentiality."),
    protects([
        DataAsset(name("Patient_Records_Database")),
        DataAsset(name("Lab_Test_Results_Data")),
        DataAsset(name("Radiology_Imaging_Data"))
    ]),
    addresses([
        SecurityProperty(name("Confidentiality"))
    ])
)

SecurityControl(
    name("Backup_Disaster_Recovery"),
    controlType("Security Process"),
    description("Automates the backup process and enables quick recovery in case of a data breach or system
failure."),
    protects([
        DataAsset(name("Patient_Records_Database")),
        Asset(name("Backup_Server")),
        Asset(name("HIS_Server"))
    ]),
    addresses([
        SecurityProperty(name("Availability"))
    ])
)

SecurityControl(
    name("Intrusion_Detection_and_Prevention_System"),
    controlType("Software"),
    description("Monitors network traffic for unusual or malicious activity and takes action to prevent potential
breaches."),
    protects([
        NetworkAsset(name("Core_Data_Center_Network")),
        NetworkAsset(name("Radiology_VLAN_60")),
        Asset(name("Security_Server"))
    ]),
    addresses([
        SecurityProperty(name("Integrity")),
        SecurityProperty(name("Confidentiality"))
    ])
)

SecurityControl(
  name("Physical_Access_Control"),
  controlType("Physical"),
  description("Secures access to critical areas, such as the Data Center and Radiology Department, using biometric scanners and RFID-enabled locks."),
  protects([
    HardwareAsset(name("Data_Center_Room")),
    HardwareAsset(name("Radiology_Imaging_Equipment")),
    HardwareAsset(name("Backup_Server"))
  ]),
  addresses([
    SecurityProperty(name("Integrity")),
    SecurityProperty(name("Confidentiality"))
  ])
)
```

```
SecurityProperty(
  name("Confidentiality_of_Patient_Records"),
  category("Confidentiality"),
  verification("Monitoring"),
  specification("Patient records must only be accessible to authorized personnel using role-based access controls and encrypted connections."),
  requiredOf([
    DataAsset(name("Patient_Records_Database")),
    Asset(name("HIS_Server"))
  ])
)

SecurityProperty(
  name("Availability_of_Laboratory_Systems"),
  category("Availability"),
  verification("Testing"),
  specification("Laboratory systems must operate continuously with a maximum allowed downtime of 10 minutes per month."),
  requiredOf([
    Asset(name("Laboratory_Information_System")),
    DataAsset(name("Lab_Test_Results_Data"))
  ])
)

SecurityProperty(
  name("Integrity_of_Administrative_Records"),
  category("Integrity"),
  verification("Static Analysis"),
  specification("Administrative records must not be modified without explicit authorization and must be validated for accuracy."),
  requiredOf([
    DataAsset(name("Administrative_Records")),
    Asset(name("Administrative_Server"))
  ])
)

SecurityProperty(
  name("Privacy_of_Medical_Imaging_Data"),
  category("Privacy"),
  verification("Inspection"),
  specification("Medical imaging data must be anonymized when shared externally and securely stored
within the hospital infrastructure."),
  requiredOf([
    DataAsset(name("Radiology_Imaging_Data")),
    Asset(name("PACS_Server"))
  ])
)

SecurityProperty(
  name("Availability_of_Network_Infrastructure"),
  category("Availability"),
  verification("Monitoring"),
  specification("The hospital's network infrastructure must ensure 99.9% uptime to support critical
healthcare operations."),
  requiredOf([
    NetworkAsset(name("DMZ_Network")),
    NetworkAsset(name("Core_Data_Center_Network"))
  ])
)

SecurityProperty(
  name("Confidentiality_of_VPN_Communications"),
  category("Confidentiality"),
  verification("Testing"),
  specification("All VPN communications must be encrypted using industry-standard encryption protocols
such as AES-256."),
  requiredOf([
    NetworkAsset(name("VPN_Network")),
    Asset(name("VPN_Server"))
  ])
)

SecurityProperty(
  name("Integrity_of_Radiology_Data"),
  category("Integrity"),
  verification("What-if Analysis"),
  specification("Radiology data must not be altered during transmission or storage."),
  requiredOf([
    DataAsset(name("Radiology_Imaging_Data")),
    Asset(name("Radiology_Server"))
  ])
)

SecurityProperty(
  name("Availability_of_Backup_Systems"),
  category("Availability"),
  verification("Monitoring"),
  specification("Backup systems must ensure that all critical data can be restored within 15 minutes in the
event of a failure."),
  requiredOf([
    Asset(name("Backup_Server")),
    DataAsset(name("Patient_Records_Database"))
  ])
)
```

5.2.3 Cyber Range Simulation and Training (CRST) Models - Training Programmes

5.2.3.1 Scenario 1: Social Engineering

The CRST Model and its sub-models for the first scenario of Pilot 2, specified using the defined language, are presented below:

```
TrainingProgramme(
  name("Social_Engineering_Training"),
  description("A structured training programme to educate hospital personnel on identifying, avoiding, and mitigating social engineering tactics such as phishing or pretexting."),
  goal("Enhance the ability of personnel to identify and prevent at least 80% of social engineering attempts targeting sensitive systems."),
  role(["Administrative Staff", "IT Personnel", "Healthcare Professionals"]),
  type("Awareness and Response"),
  legalFramework("General Data Protection Regulation (GDPR), NIS Directive, HIPAA"),
  difficulty("3"),  // Medium difficulty
  covers([
    Asset(name("PAGNI_Data_Center")),
    DataAsset(name("Patient_Records_Database"))
  ]),
  covers([
    Threat(name("Phishing_Attack")),
    Threat(name("Impersonation_Attempt"))
  ]),
  covers([
    SecurityProperty(name("Confidentiality_of_Patient_Records")),
    SecurityProperty(name("Integrity_of_Administrative_Records"))
  ]),
  covers([
    SecurityControl(name("Multi-Factor_Authentication")),
  ]),
  records([
    Trace(
      name("Social_Engineering_Trace"),
      description("A detailed log of participant activities during the training, including email analysis, verbal interaction response, and reporting actions."),
      steps([
        "Trainee receives a simulated phishing email and/or a suspicious phone call.",
        "Trainee identifies phishing or social engineering indicators (e.g., urgency tone, suspicious requests).",
        "Trainee reports the phishing attempt or impersonation to IT security."
      ]),
      feedback([
        "Correct identification of phishing or social engineering tactics.",
        "Missed indicators (e.g., urgency tone, unexpected attachments)."
      ]),
      outcomes([
        "Reported phishing or impersonation attempt flagged.",
        "Unauthorized access attempt prevented."
      ])
    )
  ]),
  supports([
    TrainingProgrammeExecution(
      name("Social_Engineering_Programme_Execution"),
      accountRole(["IT Security Specialist", "Healthcare Administrator"]),
      followedBy([
        Account(name("Admin_Account")),
        Account(name("IT_Security_Account"))
      ]),
      utilizedBy([
        Person(name("xxxxxx"), surname("xxxxxx")),
        Person(name("xxxxxx"), surname("xxxxxx"))
      ])
    )
  ]),
  consistsOf([
    Phase(
      name("Phishing_Attack_Detection"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Phishing_Attack"))
    ),
    Phase(
      name("Impersonation_Response"),
      orderOfExecution("2"),
      isBasedOn(EventSequence(name("Impersonation_Attempt"))
    )
  ]),
  contains([
    SimulationModel(name("Social_Engineering_Simulation_Model"))
  ]),
  includes([
    EmulationModel(name("Social_Engineering_Emulation_Model"))
  ])
)
```

```
Simulation(
  name("Social_Engineering_Simulation_Model"),
  description("A simulation model designed to replicate the behavior of an email server, administrative
network, and user interaction to simulate and respond to social engineering attempts."),
  deploymentMode("pre-set"),
  tool("OMNeT++"),
  executionSpeed("x2"),
  randomSeed("67890"),
  message([
    "Simulated phishing email sent to user",
    "User response logged",
    "Phishing detection and alert triggered"
  ]),
  initialization("Initialize simulation environment with OMNeT++ pre-configured network templates"),
  isPartOf(TrainingProgramme(name("Social_Engineering_Training"))),
  has([
    Phase(
      name("Phishing_Attack_Simulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Phishing_Attack"))
    )
  ]),
  simulates([
    Asset(name("Email_Server")),
   NetworkAsset(name("Administrative_Network_VLAN_90"))
]),
consistsOf([
   CompoundModule(
      name("Email_Server_Module"),
      parameters([
         "maxConnections: 200",
         "encryption: TLS 1.3"
      ]),
      properties([
         "performanceMetrics: response time, email throughput",
         "visualization: enabled"
      ]),
      consistsOf([
         SimpleModule(
            name("SMTP_Handler"),
            handles([
               "Simulated phishing email",
               "Legitimate email"
            ])
         ),
         SimpleModule(
            name("Spam_Filter_Module"),
            handles([
               "Flag phishing email",
               "Allow safe email"
            ])
         )
      ])
   ),
   CompoundModule(
      name("Network_Switch_Module"),
      parameters([
         "bandwidth: 10Gbps",
         "latency: 2ms"
      ]),
      properties([
         "performanceMetrics: packet processing rate, error rate",
         "visualization: disabled"
      ]),
      consistsOf([
         SimpleModule(
            name("Packet_Analyzer"),
            handles([
               "Incoming packets from email server",
               "Outgoing packets to user network"
            ])
         )
      ])
   )
]),
supports([
   Connection(
      name("Email_Server_to_Switch"),
      parameters([
         "protocol: SMTP",
        "encryption: TLS 1.3"
      ]),
      properties([
        "delay: 1ms",
        "datarate: 1Gbps"
      ]),
      behaviour("Bidirectional communication"),
      isPartOf(CRSTSimulationModel(name("Phishing_Simulation_Model")))
    )
  ])
)
```

```
Emulation(
  name("Social_Engineering_Emulation_Model"),
  description("An emulation model designed to replicate the email server and its interactions with both
virtual network components and external systems to enable effective phishing detection and response
training."),
  deploymentMode("pre-set"),
  tool("OpenStack"),
  initialization("Instantiate and configure email server, spam filter, and network components using
OpenStack."),
  isPartOf(TrainingProgramme(name("Social_Engineering_Training"))),
  has([
    Phase(
      name("Phishing_Email_Emulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Phishing_Attack"))
    )
  ]),
  emulates([
    SoftwareAsset(name("Email_Server")),
    SoftwareAsset(name("Spam_Filter_Service"))
  ]),
  involves([
    SoftwareAsset(name("SMTP_Service")),
    SoftwareAsset(name("Spam_Filter_Service"))
  ]),
  supports([
    VirtualNetworkModule(
      name("Phishing_Email_Network"),
      connectionAsset([
        VirtualNetworkAdapter(
          IpInfo("Static", "10.10.10.10", "255.255.255.0"),
          MAC("02:42:ac:10:00:02"),
          Routing("Default Gateway: 10.10.10.1"),
          NetPort("Port 25", "TCP", "Open")
        ),
        VirtualNetworkAdapter(
          IpInfo("Static", "10.10.10.11", "255.255.255.0"),
          MAC("02:42:ac:10:00:03"),
          Routing("Default Gateway: 10.10.10.1"),
          NetPort("Port 443", "TCP", "Open")
        )
      ])
    )
  ])
)
```

5.2.3.2 Scenario 2: Ransomware Attack on Critical Systems

The CRST Model and its sub-models for the second scenario of Pilot 2, specified using the defined language, are presented below:

```
TrainingProgramme(
  name("Ransomware_Attack_Training"),
  description("A structured training programme designed to equip IT personnel and system administrators
with the skills to identify, mitigate, and respond to ransomware attacks targeting critical hospital systems."),
  goal("Successfully detect and isolate ransomware activity while ensuring continuity of critical systems."),
  role(["IT Personnel", "System Administrators"]),
  type("Detection and Mitigation"),
  legalFramework("General Data Protection Regulation (GDPR), Network and Information Systems (NIS)
Directive"),
  difficulty("4"),  // Medium-to-high difficulty
  covers([
    Asset(name("PACS_Server")),
    Asset(name("Laboratory_Information_System")),
    DataAsset(name("Patient_Records_Database"))
  ]),
  covers([
    Threat(name("Ransomware_Attack"))
  ]),
  covers([
    SecurityProperty(name("Integrity_of_Critical_Systems")),
    SecurityProperty(name("Availability_of_Patient_Data"))
  ]),
  covers([
    SecurityControl(name("Network_Firewall_Protection")),
    SecurityControl(name("Intrusion_Detection_and_Prevention_System")),
    SecurityControl(name("Backup_Disaster_Recovery"))
  ]),
  records([
    Trace(
      name("Ransomware_Incident_Trace"),
      description("A comprehensive log of participant activities during the training, such as ransomware
detection, isolation, and restoration of systems."),
      steps([
        "Trainee identifies suspicious encrypted files in PACS server logs.",
        "Trainee isolates the affected systems from the network.",
        "Trainee restores encrypted files using backup mechanisms."
      ]),
      feedback([
        "Correct identification of ransomware activity.",
        "Effectiveness in isolating affected systems.",
        "Efficiency in restoring critical data."
      ]),
      outcomes([
        "Successful containment of ransomware spread.",
        "Critical data restored with minimal downtime."
      ])
    )
```

```
   ]),
   supports([
      TrainingProgrammeExecution(
         name("Ransomware_Programme_Execution"),
         accountRole(["IT Security Specialist", "System Administrator"]),
         followedBy([
            Account(name("IT_Admin_Account")),
            Account(name("Backup_Admin_Account"))
         ]),
         utilizedBy([
            Person(name("xxxxxx"), surname("xxxxxx")),
            Person(name("xxxxxx"), surname("xxxxxx"))
         ])
      )
   ]),
   consistsOf([
      Phase(
         name("Ransomware_Detection_Phase"),
         orderOfExecution("1"),
         isBasedOn(EventSequence(name("Ransomware_Activity_Detection"))
      ),
      Phase(
         name("System_Isolation_Phase"),
         orderOfExecution("2"),
         isBasedOn(EventSequence(name("System_Isolation_Process"))
      ),
      Phase(
         name("Data_Restoration_Phase"),
         orderOfExecution("3"),
         isBasedOn(EventSequence(name("Data_Restoration_Process"))
      )
   ]),
   contains([
      SimulationModel(name("Ransomware_Simulation_Model"))
   ]),
   includes([
      EmulationModel(name("Ransomware_Emulation_Model"))
   ])
)
```

```
Simulation(
   name("Ransomware_Simulation_Model"),
   description("A simulation model designed to replicate the behavior of ransomware attacks on critical
hospital systems, including file encryption, lateral movement, and response strategies."),
   deploymentMode("pre-set"),
   tool("OMNeT++"),
   executionSpeed("x2"),
   randomSeed("67890"),
   message([
      "Ransomware attack initiated on PACS server.",
      "Files encrypted and access blocked.",
      "Malicious activity detected by Endpoint Detection and Response (EDR) tool."
   ]),
   initialization("Initialize simulation environment with OMNeT++ configuration files and ransomware attack
templates."),
isPartOf(TrainingProgramme(name("Ransomware_Attack_Training"))),
has([
  Phase(
    name("Ransomware_Attack_Simulation_Phase"),
    orderOfExecution("1"),
    isBasedOn(EventSequence(name("Ransomware_Activity"))
  )
]),
simulates([
  Asset(name("PAGNI_Main_Server")),
  Asset(name("PAGNI_Data_Center")),
  DataAsset(name("Patient_Records_Database"))
]),
consistsOf([
  CompoundModule(
    name("PAGNI_Main_Server_Module"),
    parameters([
      "maxConnections: 200",
      "encryption: AES-256"
    ]),
    properties([
      "performanceMetrics: latency, encryption rate",
      "visualization: enabled"
    ]),
    consistsOf([
      SimpleModule(
        name("Ransomware_Payload_Handler"),
        handles([
          "File encryption activity",
          "Unauthorized access attempts"
        ])
      ),
      SimpleModule(
        name("EDR_Alert_Module"),
        handles([
          "Real-time alert generation",
          "Response activity logging"
        ])
      )
    ])
  ),
  CompoundModule(
    name("Network_Switch_Module"),
    parameters([
      "bandwidth: 1Gbps",
      "latency: 10ms"
    ]),
    properties([
      "performanceMetrics: data rate, packet loss",
      "visualization: disabled"
    ]),
    consistsOf([
      SimpleModule(
        name("Packet_Processor"),
        handles([
          "Incoming data packets",
                        "Outgoing data packets"
                    ])
                )
            ])
        )
    ]),
    supports([
        Connection(
            name("PAGNI_Main_Server_to_Network_Switch"),
            parameters([
                "protocol: SMB",
                "encryption: AES"
            ]),
            properties([
                "delay: 5ms",
                "datarate: 1Gbps"
            ]),
            behaviour("Bidirectional communication for file transfer"),
            isPartOf(CRSTSimulationModel(name("Ransomware_Simulation_Model")))
        )
    ])
)
```

```
Emulation(
    name("Ransomware_Emulation_Model"),
    description("An emulation model designed to replicate critical systems, including the PACS server and Laboratory Information System, to simulate ransomware attacks and response actions in a high-fidelity environment."),
    deploymentMode("pre-set"),
    tool("OpenStack"),
    initialization("Instantiate and configure PACS server, LIS, and backup systems using OpenStack."),
    isPartOf(TrainingProgramme(name("Ransomware_Attack_Training"))),
    has([
        Phase(
            name("Ransomware_Emulation_Phase"),
            orderOfExecution("1"),
            isBasedOn(EventSequence(name("Ransomware_Activity"))
        )
    ]),
    emulates([
        SoftwareAsset(name("PACS_Server")),
        SoftwareAsset(name("LIS"))
    ]),
    involves([
        Asset(name("Backup_Service")),
        Asset(name("PAGNI_Main_Server"))
    ]),
    supports([
        VirtualNetworkModule(
            name("Critical_Systems_Network"),
            connectionAsset([
                VirtualNetworkAdapter(
                    IpInfo("Static", "192.168.10.10", "255.255.255.0"),
                    MAC("02:42:ac:10:00:04"),
                    Routing("Default Gateway: 192.168.10.1"),
               NetPort("Port 445", "TCP", "Open")
            ),
            VirtualNetworkAdapter(
               IpInfo("Static", "192.168.10.11", "255.255.255.0"),
               MAC("02:42:ac:10:00:05"),
               Routing("Default Gateway: 192.168.10.1"),
               NetPort("Port 135", "TCP", "Open")
            )
         ])
      )
   ])
)
```

5.2.3.3 Scenario 3: System Configuration and Secure Healthcare Services

The CRST Model and its sub-models for the third scenario of Pilot 2, specified using the defined language, are presented below:

```
TrainingProgramme(
   name("Secure_System_Configuration_Training"),
   description("A training programme designed to develop the skills required for securely configuring critical
healthcare systems and ensuring the continuous delivery of secure services."),
   goal("Achieve a secure configuration baseline for critical systems and ensure compliance with security
policies."),
   role(["IT Personnel", "System Administrators"]),
   type("Configuration and Hardening"),
   legalFramework("General Data Protection Regulation (GDPR), NIS Directive"),
   difficulty("3"),  // Medium difficulty
   covers([
      Asset(name("HIS_Server")),
      Asset(name("LIS")),
      DataAsset(name("Patient_Records_Database"))
   ]),
   covers([
      Threat(name("Misconfigured_System_Exploitation")),
   ]),
   covers([
      SecurityProperty(name("Integrity_of_System_Configuration")),
      SecurityProperty(name("Confidentiality_of_Patient_Data"))
   ]),
   covers([
      SecurityControl(name("Network_Firewall_Protection")),
      SecurityControl(name("Role-Based_Access_Control"))
   ]),
   records([
      Trace(
         name("System_Configuration_Trace"),
         description("A detailed log of participant activities during the training, including configuration changes,
testing, and verification."),
         steps([
            "Trainee analyzes existing system configurations for vulnerabilities.",
            "Trainee updates configurations based on security best practices.",
            "Trainee tests and verifies the updated configurations."
         ]),
         feedback([
        "Identified misconfigurations and suggested corrections.",
        "Accuracy of updated configurations.",
        "Effectiveness of testing and verification processes."
      ]),
      outcomes([
        "Critical systems hardened against potential threats.",
        "Reduced risk of unauthorized access or data breaches."
      ])
    )
  ]),
  supports([
    TrainingProgrammeExecution(
      name("Configuration_Programme_Execution"),
      accountRole(["System Administrator", "IT Security Specialist"]),
      followedBy([
        Account(name("Admin_Account")),
        Account(name("Config_Manager_Account"))
      ]),
      utilizedBy([
        Person(name("xxxxxx"), surname("xxxxxx")),
        Person(name("xxxxxx"), surname("xxxxxx"))
      ])
    )
  ]),
  consistsOf([
    Phase(
      name("System_Configuration_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Configuration_Analysis"))
    ),
    Phase(
      name("Configuration_Hardening_Phase"),
      orderOfExecution("2"),
      isBasedOn(EventSequence(name("System_Hardening"))
    ),
    Phase(
      name("Configuration_Verification_Phase"),
      orderOfExecution("3"),
      isBasedOn(EventSequence(name("Testing_and_Verification"))
    )
  ]),
  contains([
    SimulationModel(name("Configuration_Simulation_Model"))
  ]),
  includes([
    EmulationModel(name("Configuration_Emulation_Model"))
  ])
)
```

```
Simulation(
  name("Configuration_Simulation_Model"),
  description("A simulation model designed to replicate system configuration scenarios, including identifying vulnerabilities, applying secure configurations, and verifying compliance with security standards."),
  deploymentMode("pre-set"),
  tool("OMNeT++"),
  executionSpeed("x1"),
  randomSeed("54321"),
  message([
    "System configuration analyzed for vulnerabilities.",
    "Secure configuration settings applied.",
    "Verification of updated configurations completed."
  ]),
  initialization("Initialize simulation environment with pre-configured OMNeT++ templates for system
configuration scenarios."),
  isPartOf(TrainingProgramme(name("Secure_System_Configuration_Training"))),
  has([
    Phase(
      name("Configuration_Analysis_Simulation_Phase"),
      orderOfExecution("1"),
      isBasedOn(EventSequence(name("Configuration_Analysis"))
    ),
    Phase(
      name("Configuration_Hardening_Simulation_Phase"),
      orderOfExecution("2"),
      isBasedOn(EventSequence(name("System_Hardening"))
    ),
    Phase(
      name("Configuration_Verification_Simulation_Phase"),
      orderOfExecution("3"),
      isBasedOn(EventSequence(name("Testing_and_Verification"))
    )
  ]),
  simulates([
    Asset(name("HIS")),
    SoftwareAsset(name("LIS ")),
    DataAsset(name("Patient_Records_Database")),
    DataAsset(name("Network_Configuration_Data")),
  ]),
  consistsOf([
    CompoundModule(
      name("HIS_Server_Module"),
      parameters([
        "maxConnections: 100",
        "encryption: Enabled (TLS 1.3)"
      ]),
      properties([
        "performanceMetrics: configuration change time, error rate",
        "visualization: enabled"
      ]),
      consistsOf([
        SimpleModule(
          name("Configuration_Analyzer"),
          handles([
            "Analyze system configuration vulnerabilities",
            "Identify misconfigured settings"
          ])
        ),
        SimpleModule(
          name("Configuration_Updater"),
          handles([
            "Apply secure configuration settings",
                  "Generate configuration update logs"
               ])
            )
         ])
      ),
      CompoundModule(
         name("Network_Switch_Module"),
         parameters([
            "bandwidth: 1Gbps",
            "latency: 5ms"
         ]),
         properties([
            "performanceMetrics: data flow consistency, packet loss rate",
            "visualization: disabled"
         ]),
         consistsOf([
            SimpleModule(
               name("Packet_Validator"),
               handles([
                  "Verify data packets adhere to updated configurations",
                  "Log configuration verification details"
               ])
            )
         ])
      )
   ]),
   supports([
      Connection(
         name("HIS_Server_to_Switch"),
         parameters([
            "protocol: HTTPS",
            "encryption: TLS 1.3"
         ]),
         properties([
            "delay: 2ms",
            "datarate: 1Gbps"
         ]),
         behaviour("Bidirectional communication for configuration updates"),
         isPartOf(CRSTSimulationModel(name("Configuration_Simulation_Model")))
      )
   ])
)
```

```
Emulation(
   name("Configuration_Emulation_Model"),
   description("An emulation model designed to replicate the critical systems, including the HIS server and
Laboratory Information System, to simulate secure configuration processes and validate the applied changes
in a high-fidelity environment."),
   deploymentMode("pre-set"),
   tool("OpenStack"),
   initialization("Instantiate and configure HIS server, LIS, and network components using OpenStack."),
   isPartOf(TrainingProgramme(name("Secure_System_Configuration_Training"))),
   has([
      Phase(
         name("Configuration_Analysis_Emulation_Phase"),
         orderOfExecution("1"),
         isBasedOn(EventSequence(name("Configuration_Analysis"))
      ),
      Phase(
         name("Configuration_Hardening_Emulation_Phase"),
         orderOfExecution("2"),
         isBasedOn(EventSequence(name("System_Hardening"))
      ),
      Phase(
         name("Configuration_Verification_Emulation_Phase"),
         orderOfExecution("3"),
         isBasedOn(EventSequence(name("Testing_and_Verification"))
      )
   ]),
   emulates([
      SoftwareAsset(name("HIS")),
      SoftwareAsset(name("LIS"))
   ]),
   involves([
      SoftwareAsset(name("Configuration_Management_Tool")),
      SoftwareAsset(name("Network_Configuration_Service"))
   ]),
   supports([
      VirtualNetworkModule(
         name("Configuration_Network"),
         connectionAsset([
            VirtualNetworkAdapter(
               IpInfo("Static", "192.168.20.10", "255.255.255.0"),
               MAC("02:42:ac:20:00:04"),
               Routing("Default Gateway: 192.168.20.1"),
               NetPort("Port 443", "TCP", "Open")
            ),
            VirtualNetworkAdapter(
               IpInfo("Static", "192.168.20.11", "255.255.255.0"),
               MAC("02:42:ac:20:00:05"),
               Routing("Default Gateway: 192.168.20.1"),
               NetPort("Port 22", "TCP", "Open")
            )
         ])
      )
   ])
)
```

6 Conclusions

This deliverable, **D3.2: "AERAS Models and CRSA-driven Cyber Range Programme V1,"** represents a significant milestone in the development of the AERAS platform and forms the cornerstone of Work Package 3 (WP3). It marks the completion of the first version of the CRSA models and the CRSA-driven Cyber Range Training (CRST) programs, specifically tailored to address the unique cybersecurity requirements of the two pilot organizations participating in the AERAS project.

The deliverable begins by presenting the pilot environment architectures, detailing their operational contexts, infrastructure setups, and relevant cybersecurity requirements. This is followed by an in-depth analysis of the threat landscapes and the training program specifications for the **Smart Hospital Environment pilot** (Pilot 1) and the **Healthcare Authority pilot** (Pilot 2). Leveraging this foundational analysis, the defined and developed CRSA models and CRST training programs are introduced, providing an overview of their structure, objectives, and alignment with the needs of the pilot organizations.

This work is closely aligned with and highly dependent on **Deliverable D5.3: "AERAS Initial Prototype Pilot Validation Report"**, which directly informs the requirements and cybersecurity training needs of the pilots, as identified through stakeholder engagement and risk analysis. By integrating the insights from D5.3, this deliverable ensures that the developed models and training programs are both relevant and effective for the participating organizations.

The CRSA models and CRST training programs detailed in this deliverable are not static; they will undergo rigorous re-evaluation and refinement during the two validation rounds of the AERAS pilots. This iterative process ensures continuous improvement and adaptation to the evolving needs and feedback of the pilot organizations. The final version of the CRSA-driven Cyber Range Program, incorporating all lessons learned and refinements, will be presented in Deliverable **D3.3: "AERAS Models and CRSA-driven Cyber Range Programme V2"**.

The work performed in D3.2 establishes a strong foundation for subsequent deliverables and future activities within Work Package 3 (WP3). By defining the initial version of the CRSA-driven Cyber Range Programs, this deliverable provides a roadmap for enhancing and finalizing the CRSA models and CRST training programs that will ultimately implement and validate the two AERAS pilots. The insights and methodologies outlined here play a pivotal role in achieving the objectives of the AERAS project, ensuring the platform’s effectiveness in addressing real-world cybersecurity challenges within the healthcare sector.

7 References

[1] I. O. f. Standardization, “ISO/IEC 27000 Family Information Security Management,” 2024. [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accessed 2024].

[2] I. S. Organization, “ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls,” 2022. [Online]. Available: https://www.iso.org/standard/75652.html. [Accessed 2024].

[3] I. S. Organization, “ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,” 2019. [Online]. Available: https://www.iso.org/standard/76559.html. [Accessed 2024].

[4] I. S. Organization, “ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security,” 2023. [Online]. Available: https://www.iso.org/standard/76070.html. [Accessed 2024].

[5] NIST, “NIST Cybersecurity Framework,” 2024. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 2024].

[6] NIST, “SP 800-53 Rev.4 - Security and Privacy Controls for Federal Information Systems and Organizations,” NIST, 2013. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r4/upd3/final. [Accessed 2024].

[7] NIST, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” 2018. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/final. [Accessed 2024].

[8] E. Union, “General Data Protection Regulation (GDPR),” 2018. [Online]. Available: https://gdpr-info.eu/. [Accessed 2024].

[9] ISACA, “COBIT, Control Objectives for Information Technologies,” 2020. [Online]. Available: https://www.isaca.org/resources/cobit. [Accessed 2024].

[10] P. A. Networks, “What is Zero Trust Architecture (ZTA),” 2024. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture. [Accessed 2024].

[11] O. Foundation, “OWASP Top Ten,” 2024. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 2024].

[12] I. S. Organization, “Health informatics — Information security management in health using ISO/IEC 27002,” 2016. [Online]. Available: https://www.iso.org/standard/62777.html. [Accessed 2024].

[13] HITRUST, “Health Information Trust Alliance Cybersecurity Framework (HITRUST) CSF — Our Framework,” 2024. [Online]. Available: https://hitrustalliance.net/hitrust-framework. [Accessed 2024].

[14] CDC, “Health Insurance Portability and Accountability Act of 1996 (HIPAA),” 1996. [Online]. Available: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html. [Accessed 2024].

[15] HHS, “Health Information Technology for Economic and Clinical Health (HITECH) Act Enforcement Interim Final Rule,” 2009. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html. [Accessed 2024].

[16] NIST, “NIST Updates Guidance for Health Care Cybersecurity,” 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity. [Accessed 2024].

[17] I. S. Organization, “ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security,” 2022. [Online]. Available: https://www.iso.org/standard/72891.html. [Accessed 2024].

[18] E. Union, “EUCC - The EU Cybersecurity Certification Framework,” 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. [Accessed 2024].

[19] ENISA, “Cyber Security and Resilience for Smart Hospitals,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.

[20] AICPA, “SOC 2 Type 2 Compliance for Service Organizations,” 2024. [Online]. Available: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2. [Accessed 2024].

[21] IBM, “What is the IT Infrastructure Library (ITIL)?,” 2024. [Online]. Available: https://www.ibm.com/think/topics/it-infrastructure-library. [Accessed 2024].

[22] CONCORDIA, “Deliverable D3.3: 3rd Year Report on Community Building and Sustainability,” 2021. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D3.3.pdf. [Accessed 2024].