VILNIUS UNIVERSITY

KAUNAS FACULTY

INSTITUTE OF SOCIAL SCIENCES AND APPLIED INFORMATICS

SEATS: Social Engineering Awareness Training System for Employees in Organizations

Work by: ISCS student Anton Klymchuk

Submitted to: P'Ship Prof., Dr. Darius Dilijonas

Kaunas 2025

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

INTRODUCTION

Relevance:

Social engineering attacks continue to concern organizations of all kinds. Malicious hackers use these attacks to target one of the weakest elements of an information system: users. Social engineering attacks take many forms but have the same goal: to trap users into performing activities they might otherwise never do. Social engineering attacks, such as phishing, pretexting, and baiting pose a significant threat to organizations (Kirvan, 2025).

Employees are often the weakest and most vulnerable link in the cybersecurity state of the organization due to a list of factors: unawareness of malicious actions on the Internet, lack of knowledge of cyber threats, lack of focus and attention. These factors emphasize how crucial it is to train the employees on recognizing and preventing different types of threats, including social engineering attacks. A structured awareness training system should ensure that employees stay informed about cyber threats, such as social engineering, and should help to reduce security breaches caused by human error.

Problem:

Despite increasing investments in cybersecurity infrastructure, organizations struggle with social engineering attacks because employees remain the weakest link in security. Many organizations lack structured and engaging training programs to educate employees on recognizing and responding to social engineering threats (Bill Gardner and Valerie Thomas, 2014). Organizations face challenges in managing cybersecurity awareness among the employees due to:

1. Limited engagement in traditional security awareness methods (e.g., slideshows, PDFs) ineffectively engage employees into learning process (Bill Gardner and Valerie Thomas, 2014).
2. Lack of contextualization, meaning training content is often generic and does not address industry-specific, company-specific, or role-specific cyber threats and risks (Bill Gardner and Valerie Thomas, 2014).
3. Many awareness training methods lack interactive assessments and progress tracking of employees (Bill Gardner and Valerie Thomas, 2014).
4. Lack of structured training or a knowledgebase on social engineering threats.
5. Inconsistent enforcement of employee participation in cybersecurity awareness training programs.
6. Growing need for a contextualized, interactive, structured training approach.

Proposed solution:

The Social Engineering Awareness Training System should provide:

- A structured training program.
- Studying material and assessments to measure understanding.
- Progress tracking to ensure participation.
- A centralized platform for ongoing social engineering awareness education.

This system should help organizations effectively reduce human-related security risks.

Purpose:

To develop a web-based social engineering awareness training system that educates employees about cyber threats contextualized to the organization activities and tests their awareness through interactive modules.

Object:

An organization implementing social engineering awareness training.

Tasks:

1. Analyze social engineering concept, types and impact of social engineering attacks
2. Analyze existing awareness training methods and web-based information systems.
3. Define requirements for the system based on performed analysis.
4. Design the system architecture and key features.
5. Implement core functionalities such as training modules and quizzes.

Main functions/features:

- **User authentication:** Employees log in to access training.
- **Training modules:** Interactive lessons on phishing, business email compromise, ransomware etc.
- **Assessment:** Multiple-choice assessments to test knowledge.
- **Progress tracking:** Users can track completion rates and scores.
- **Reporting and analytics:** Admins can generate reports on training effectiveness.

Users:

- **Employees:** Primary users who take training and assessments.
- **Administrators (IT/Security team):** Manage content, monitor progress, and generate reports.

1. ANALYSIS

1.1 General characteristics of Social Engineering. Understanding the domain field.

1.1.1 What is Social Engineering.

Social engineering is an attack vector that relies on human weakness. An attack has a simple goal: to enable the attacker to bypass security; gain unauthorized access to systems, data or physical locations; and commit a variety of criminal activities (Kirvan, 2025).

Sophistication level and attack vectors of social engineering attacks can vary. In context of employees of organization , from a simple non-personalized email with "Click here" malicious link from unauthorized sender regarding some of organization-related services to business email compromise scams where threat actors impersonate another individual – employees or employer himself – to ask for some personal or sensitive organizational data to, for example, continue a normal workflow of some department or whole company .

This varying range of social engineering attack vectors may cause a lot of implications on the organizational workflow, as well as may lead to financial losses, data breaches, and may compromise company's reputation and integrity.

1.1.2 Types of Social Engineering attacks.

In context of selected domain field, I would like to specify most common types of social engineering attacks:

- **Phishing/smishing/vishing** — types of social engineering attacks varying between email, SMS, or calls respectively. The main idea behind these attack types is to persuade a potential victim into sharing personal identifiable data, clicking malicious links, downloading malicious files etc. Often these attacks may have urgent and persuasive context.
- **Business email compromise (BEC)** – when attacker impersonates employee's colleague or superior to gain access to sensitive data. For example, Chief Financial Officer (impersonated threat actor) asking a Senior Accountant (employee) to share financial report for the last quarter for some business needs.
- **Spear phishing** – more targeted phishing attack which involves malicious actors singling out a user or group of users to trick them into providing sensitive data or performing an

action. Spear phishing attacks are generally not random attacks, but well-researched scams.

- **Ransomware via social engineering** – while ransomware itself is a type of malware, it is often delivered through social engineering methods such as phishing. In such cases, the victim is tricked into opening a malicious attachment or link that installs ransomware, which then encrypts organizational data and demands payment to restore access. This method relies on human error and trust, making it a significant threat in corporate environments.

1.1.3 Impact of Social Engineering attacks.

The following statistics are retrieved from a conference paper "*Impact of Social Engineering Attacks: A Literature Review*" (Walter Fuertes, Diana Arévalo, Joyce Denisse Castro, Mario Ron,Carlos Andrés Estrada, Roberto Andrade, Felix Fernández Peña,and Eduardo Benavides, 2021).

Studies demonstrate that phishing and ransomware are the types of social engineering attacks with the highest impact in the world. Through fraudulent emails or fake websites, attackers take advantage of human mistakes and deceive users with messages containing offers or threats. In this way, they steal credentials and impersonate identities. Social engineering attacks significantly impact the global economy and cause serious damage to organizational reputations. In recent years, losses due to ransomware attacks have reached billions, highlighting the immense financial damage inflicted on companies.

Phishing	Ransomware
97% of users do not recognize Phishing e-mails	It has grown 350% since 2018 as a popular form of attack
95% of attacks are for companies	Ransomware detection is on the rise at 543%
Employees have trouble recognizing Phishing e-mails	81% of experts say there will be more Ransomware attacks
3% of users report Phishing attacks	E-mail Ransomware increased by 109%
30% open e-mails and 12% open the malicious link	21% of Ransomware involved social actions
81% of Phishing attacks on mobile devices have been without mail	51% of businesses have been affected by Ransomware
85% of companies have attacked at least once	Ransomware variants grew by 46% in 2019
97.25% have Ransomware	Ransomware attacks increased 41% to 205,000
78% of people have mentioned that they know the links but open it	65% of Ransomware infections are sent via Phishing
Webmail services account for 34.7% of Phishing attacks	A Ransomware attack will occur every 11s by 2021
96% of attacks are aimed for gathering information	85% of Ransomware attacks in 2019 was 133,000
71% of sextortion victims are under the age of 18	In 2019, 68,000 new Ransomware Trojans were detected
81% of all attacks are for spoofing	50% of professionals do not believe that their company is prepared for an attack
22% of all data breaches in 2020 involve Phishing attacks	90% of professionals claim to have clients who suffered Ransomware attacks

Source: *(Walter Fuertes, Diana Arévalo, Joyce Denisse Castro, Mario Ron,Carlos Andrés Estrada, Roberto Andrade, Felix Fernández Peña,and Eduardo Benavides, 2021)*. Accessed on 03/04/2025 via https://www.researchgate.net/publication/355754456_Impact_of_Social_Engineering_Attacks_A_Literature_Review

Figure 1 **Phishing versus Ransomware statistics**

1.1.4 How to prevent Social Engineering attacks.

There exist some methods to reduce such attacks' impact, from three aspects, being the detection of social engineering attacks, education, and training, as well as building the awareness towards prevention of these attacks. Employees should be cautious with suspicious emails, calls, or messages – especially those requesting sensitive data or creating a sense of urgency.

On an organizational level, companies should regularly conduct awareness training, simulate social engineering attacks and enforce policies that support security. Human is often a neglected factor, leading organizations to invest millions of dollars in implementing security technologies and applying

standards that mostly focus on technical defenses such as hardware and software. However, one of the most effective ways to mitigate social engineering attacks is through education and training of those who are most susceptible. (Walter Fuertes, Diana Arévalo, Joyce Denisse Castro, Mario Ron,Carlos Andrés Estrada, Roberto Andrade, Felix Fernández Peña,and Eduardo Benavides, 2021).

1.2 How companies approach Social Engineering Awareness trainings.

Organizations are more and more focusing on social engineering awareness training to counter the increasing number of human-oriented cyberattacks. However, the methodologies differ greatly in their approach, content, and sophistication. Below is an examination of current-day corporate practices highlighting findings from the *"2024 State of the Phish"* report (proofpoint., 2024 State of Phish \ Report, 2024).

1.2.1 Adoption of Awareness Programs.

Almost all organizations from Proofpoint's research scope have implemented some sort of security awareness training. Despite this, only 53% of companies train all employees, leaving knowledge gaps. Certain employee groups, mostly finance or IT, are trained more than others, frequently leaving behind employees from other departments. The inconsistency in engagement creates a potential vulnerability: many employees remain untrained or unprepared for targeted attacks (spear phishing, BEC, phishing).

A significant disconnect exists between security teams and employees. While 85% percent of security professionals believe that employees know their role cybersecurity, only 41% of employees admit they have this responsibility. Unfortunately, employees prefer convenience over security, leading to 70% of them admitting to actions like reusing passwords or clicking suspicious links.

1.2.2 Social Engineering Training approaches.

Companies use different formats to deliver trainings. Most of them prefer computer-based modules (45%) since they provide maximum flexibility and scalability. Interactive methods like simulated phishing attacks are less common (34%), despite they are quite effective in reproducing real-world social engineering attack scenarios. The adoption of gamification in awareness training, such as contests and prizes, has increased to 23%, showing an increased employee engagement through incentives rather than passive forms of learning. In-person and virtual training sessions are also used. However, they are often offered for some specific employee groups with specific roles.

1.2.3 Relevance of studying content.

Awareness trainings usually consists of basic knowledge on phishing, malware, ransomware, etc., with many failing to address emerging threats. For example, around 20% of companies provide company-wide training on vishing or AI-based attacks, even though these methods are becoming more common. The lack of contextualization, meaning that training does not adjust to industry-specific or company-specific risks, further decreases the effectiveness of training itself. Employees often struggle to apply generalized knowledge to situations in their workflows. This leads to increased vulnerability of employees to sophisticated attack scenarios.

1.2.4 Evaluation of awareness practices and proposed improvements.

Many organizations still rely on passive or inconsistent training approaches to educate employees about social engineering threats. Awareness training is often presented using PDF guides, monthly newsletters, or PowerPoint presentations. These methods lack interactivity and personalized learning experiences which leads to low engagement and ineffective results.

According to the *2023 KnowBe4 Phishing Benchmarking Report* (Kron, 2023), organizations that do not provide regular awareness training experience an average of 1 in 3 employees clicking on a phishing link or failing for a social engineering attempt. In comparison, organizations that implement structured training and simulated phishing saw a reduction to as low as 4.2% within a year — particularly in small organizations with under 250 employees. Indeed, this gap indicates a future improvement that can be obtained by consistent and targeted training.

The proposed system aims to improve current state of things by offering a lightweight, web-based platform that delivers interactive training modules, quizzes and progress tracking. It enables administrators to assign deadlines, monitor participation, and evaluate effectiveness — all of which are missing in many current setups.

1.3 Comparison of Security Awareness Training solutions.

To evaluate the market for the proposed social engineering awareness training system, I would like to compare it with two of the most popular existing solutions: *KnowBe4 Security Awareness Training* (KnowBe4, 2025) and *Proofpoint's ZenGuide* (proofpoint., Mitigate Human Risk, 2025) (proofpoint., Proofpoint ZenGuide, 2024). Both platforms are very well-established leaders in the domain of security awareness training and have complex features related to phishing simulation, risk analysis of users, and

customizable content. While my proposed solution is a lightweight system focused on small to medium-sized organizations, *KnowBe4* and *ZenGuide* deliver enterprise-level solutions. Below is a comparison table of the similarities and differences along with the value proposition of the compared system.

Table 1

Comparison of Security Awareness Training solutions

Feature/Aspect	SEATS	Proofpoint ZenGuide	KnowBe4
Target market	Small to medium-sized organizations seeking contextualized training	Enterprise organizations with complex security ecosystems	Organizations of all sizes, primarily enterprise
Focus	Contextualized social engineering awareness training aligned to company activities	General security awareness	Comprehensive security awareness with focus on phishing simulation
Integration complexity	Low complexity, lightweight implementation	High complexity; requires complex configuration	Medium to high complexity
Implementation cost	Low-cost solution with essential features	High-cost enterprise solution	Medium to high cost with tiered pricing
Contextualization	Industry and company-specific scenarios based on actual company workflows	Generic scenarios with some customization options	Large template library but limited company-specific contextualization
User interface	Simple interface focused on ease of use	Complex dashboard with multiple features	Feature-rich interface with moderate learning curve
Content creation	Enables admins to create company-specific content through dedicated interface	Requires professional services for customization	Template customization available but complex
Learning approach	Interactive modules with role-specific content	Varied content types with behavioral analysis	Multi-format content
Assessment methods	Practical assessments related to daily work scenarios	Knowledge tests and simulations	Knowledge tests and simulated phishing
Reporting	Reports on training effectiveness	Complex reporting with risk scoring	Extensive reporting with behavioral analytics
Unique value	Contextualized training specific to organizational workflows and employee' vulnerabilities	Threat intelligence integration and advanced analytics	Large content library and simulated phishing capabilities

To summarize, technical sophistication and scalability are not yet strengths of SEATS like they are for KnowBe4 or ZenGuide. Thus, SEATS' greatest assets are affordability, flexible customization, and contextualization of particular organizational needs. It should provide practical solution for small organizations or those in the earliest phase of building a cybersecurity awareness culture. With further stages of development and versions of proposed information system, analytics, automation, phishing

simulations, and extended content scope could be introduced into that domain, which the enterprise platforms have already mastered.

1.4 Functional and technical requirements for the proposed system.

1.4.1 Functional/Non-Functional requirements for SEATS

The aim is to rapidly build a web-based social engineering awareness training system for employees in a company that would have learning modules with study materials and assessment tests. Employees will be able to take tests, see their calculated results and track their progress. There should be a separate interface for administrators where they should have CRUD functionality. Also, admins will be able to overlook employees' success rates and add learning modules, as well as generate reports on training effectiveness.

Functional Requirements

- **User authentication and access control**
  - Users must log in using corporate email and password.
  - Passwords must follow security guidelines of minimum length, special characters.
  - Users can reset their passwords if forgotten.
- **Employee functionalities**
  - View assigned training modules (videos, text lessons, images).
  - Complete modules before gaining access to the corresponding assessment (quiz).
  - Take quizzes with predefined passing limits (e.g., 60-70% correct to pass).
  - View quiz results, including correct answers and explanations for mistakes.
  - Employees can view their overall progress (completed/pending modules).
  - Employees can retake failed quizzes after a cooldown period (configurable by Admin).
- **Admin (IT/security team) functionalities**
  - View a dashboard with employees' progress, deadlines, and quiz results.
  - Admins can monitor individual and team progress.
  - Create and manage training modules (add/edit/delete study materials).
  - Set deadlines for each module.
  - Create and edit quizzes (questions, answer choices, correct answers, passing threshold).
  - Admins overlook user accounts (add, remove, modify employees' roles).

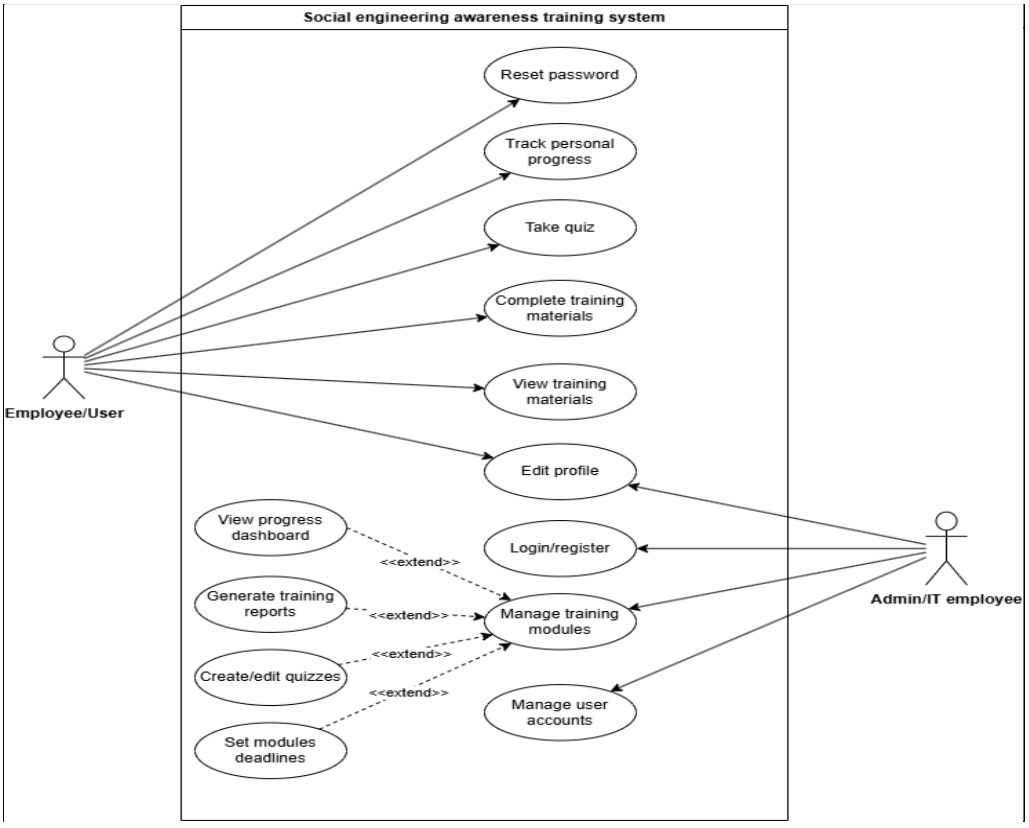
- Generate reports on training effectiveness.

- **System architecture**
  - Data is stored in a relational database (preliminary MySQL).
  - Training materials and quizzes are linked to employee accounts.
  - Admins have separate access control from employees.

Non-functional requirements

- The system must be accessible via web browser.
- It should have a simple, user-friendly interface.
- Secure authentication and role-based access control.
- System should support basic export of progress reports (PDF, csv).

I used "Claude.ai" (Anthropic, 2025) and "Mermaid" (Sveidqvist, 2025) to create a **General Use Case diagram**. I finetuned it to satisfy my requirements. Here is a prompt: "Create a use case diagram on the basis of requirements description, functional and non-functional requirements."



Source: created by author using Draw.io *(JGraph, 2023)*, Claude *(Anthropic, 2025)*, and Mermaid *(Sveidqvist, 2025)*

Figure 2 **General Use Case diagram**

1.4.2 Domain Model of SEATS

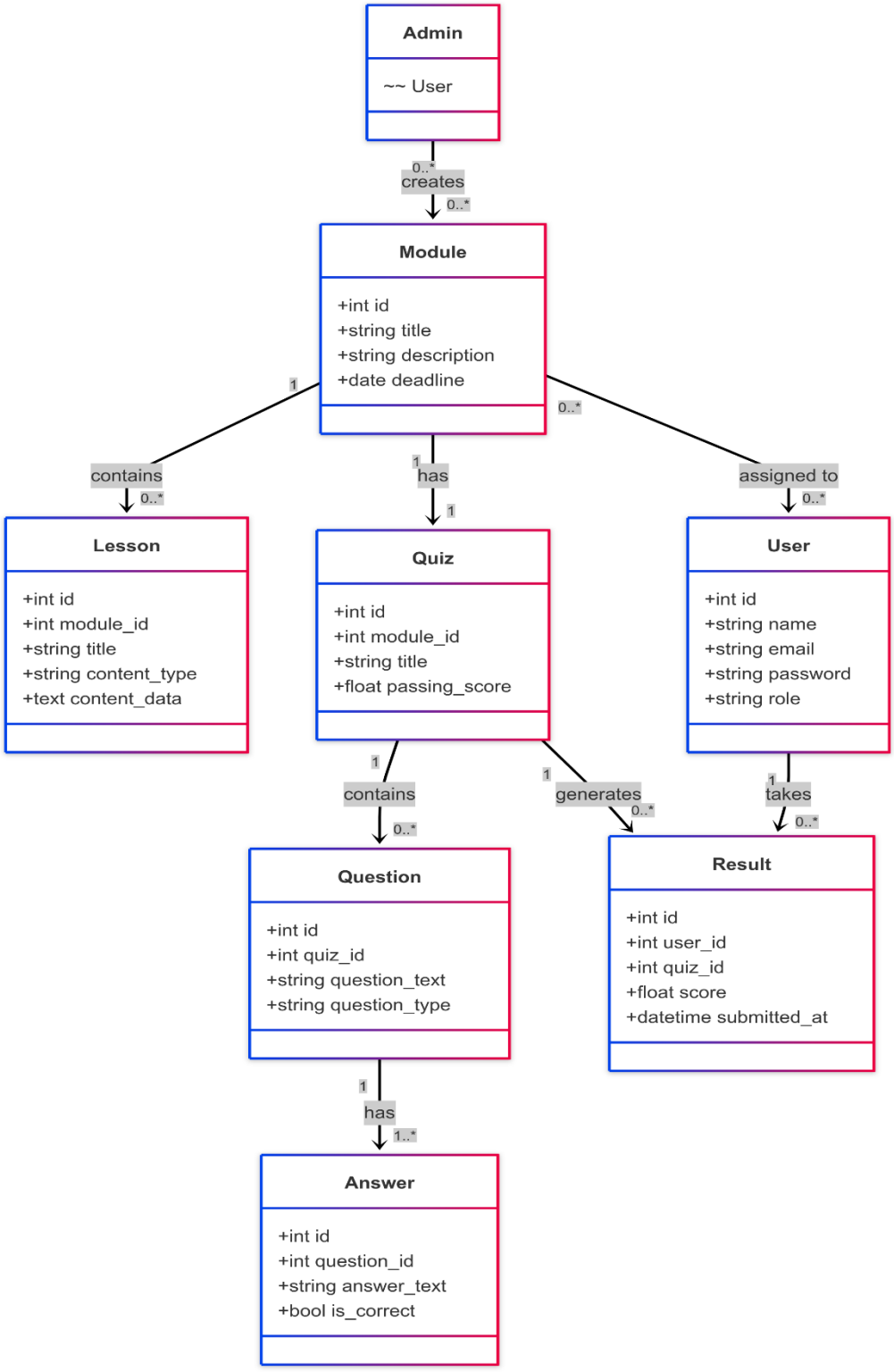
The conceptual domain model describes the main entities of proposed Social Engineering Awareness Training System (SEATS) and the relationships among them. The domain model defines how the system is meant to work at the early stages of development. Also, it sets a basis for database design and implementation.

The model reflects how system components interact to deliver structured social engineering awareness content. Main components include users, training modules, quizzes, and results. The indirect information flow within the system is: from admin assigning modules to users completing lessons and quizzes and ending with results being stored for review and tracking.

Main entities are:

- **User –** Represents any user of the system (employees). Each user has basic attributes: name, email, password, and role. Roles differentiate between normal users and admins.
- **Admin –** Inherited from User; Admins manage modules, quizzes, and monitor employee progress.
- **Modules –** The training unit to be active for a period. Admin creates modules and assigns them to users. Each module contains lessons and one quiz.
- **Lesson –** Studying content (video, text etc.) is inside the module; one module may have more than one lesson.
- **Quiz –** Set of questions to test employees' understanding of module. Every module gets one quiz attached.
- **Question –** Related to quiz, consists of multiple-choice answer types. Each question may have one or multiple possible answer choices.
- **Result –** Stores entries for submissions in the quiz, including scores, time submitted, and ID of the user. A record linking each attempt on the quiz with a user.

The relationships between these entities provides a vision of how information flows through the system. For example, admin creates module → assigns it to users → users access lessons → finish the quiz → system saves the result → admins review performance.



Source: created by author with help of Mermaid Chart *(Sveidqvist, 2025)*, ChatGPT *(OpenAI, 2025)*

Figure 3 **Domain Model**

1.4.3 Description of computerization tools.

OBLIGATORY:

- JavaScript – Used for frontend responsiveness.
- HTML/CSS – Used for structuring and styling the user interface.
- XAMPP – Local server environment for running Apache and MySQL.
- phpMyAdmin – Web-based tool for MySQL database management.
- VS Code – Integrated development environment.
- Bootstrap – Frontend framework for styling and responsive design.
- Microsoft Edge – Browser for testing system functionality.
- Draw.io – Tool for creating diagrams.
- Mermaid Chart – Tool for creating diagrams.
- AI assistance – ChatGPT, Claude, Gemini, Perplexity, Microsoft Copilot, GitHub Copilot.

OPTIONAL:

- Postman – For testing HTTP requests and possible APIs (if added later).
- PHPMailer – Library for sending system email notifications.
- Appsmith, WordPress – Alternative development approaches.
- AJAX – For sending data to the server without page reloads.

2. TECHNICAL TASK

1. **TITLE OF THE COURSE WORK.**

   SEATS: Social Engineering Awareness Training System for Employees in Organizations.

2. **CONTENT OF ANALYTICAL AND RESEARCH STUDY:**

   2.1 General characteristics of Social Engineering. Understanding the domain field.

   - 2.1.1 What is Social Engineering.
   - 2.1.2 Types of Social Engineering attacks.
   - 2.1.3 Impact of Social Engineering attacks.
   - 2.1.4 How to prevent Social Engineering attacks.

   2.2 How companies approach Social Engineering Awareness trainings.

   - 2.2.1 Adoption of Awareness Programs.
   - 2.2.2 Social Engineering Training approaches.
   - 2.2.3 Relevance of studying content.
   - 2.2.4 Evaluation of awareness practices and proposed improvements.

   2.3 Comparison of Security Awareness Training solutions.

   2.4 Functional and technical requirements for the proposed system.

   - 2.4.1 Functional/Non-Functional requirements for SEATS.
   - 2.4.2 Domain Model of SEATS.
   - 2.4.3 Description of computerization tools.

3. **FUNCTIONS OF THE DESIGNED INFORMATION SYSTEM.**

   3.1 User authentication: Employees log in to access training.

   3.2 Training modules: Interactive lessons on phishing, business email compromise, ransomware etc.

   3.3 Assessment: Multiple-choice assessments to test knowledge.

   3.4 Progress tracking: Users can track completion rates and scores.

   3.5 Reporting and analytics: Admins can generate reports on training effectiveness.

4. **SYSTEM DESCRIPTION DOCUMENTATION AND INSTRUCTIONS.**

   4.1 Employee user manual.

   4.2 Admin user manual.

   4.3 System structure overview.

5. **INFORMATION SYSTEM DESIGN AND DEVELOPMENT TOOLS. SOFTWARE AND HARDWARE REQUIREMENTS.**

5.1 Design and logic modeling tools – *Draw.io, Mermaid Chart, ChatGPT, Claude, Gemini, Microsoft Copilot, GitHub Copilot, MaricDraw 18.2 (optional).*

5.2 Frontend development tools – *HTML, CSS, JavaScript, Bootstrap, AI Assistance.*

5.3 Backend development tools – *PHP, XAMPP environment, AJAX, AI Assistance, PHPMailer (optional).*

5.4 Database management system – *MySQL, managed via phpMyAdmin.*

5.5 Development environment – *Visual Studio Code.*

5.6 System operating environment – *Windows 10 or higher (compatible with XAMPP).*

5.7 Browser for testing – *Microsoft Edge.*

5.8 Optional tools – *Postman (for API testing), Appsmith and WordPress (as alternative development platforms).*

5.9 Technical equipment requirements – *Intel Core i5-7xxx, 3.10 GHz, DDR4-SDRAM.*

6. **SYSTEM TESTING AND EVALUATION.**

6.1 Functional testing of core features such as login, module access, quiz completion, and result tracking.

6.2 Usability evaluation of user experience with a small group of users and collecting basic feedback.

7. **WORK DELIVERY REQUIREMENTS.**

7.1 Coursework description in accordance with the methodological guidelines for writing a Bachelor's thesis.

7.2 Oral presentation and pptx presentation of Coursework during the defense (6-8 min.).

3. PURPOSE OF THE INFORMATION SYSTEM PROJECT

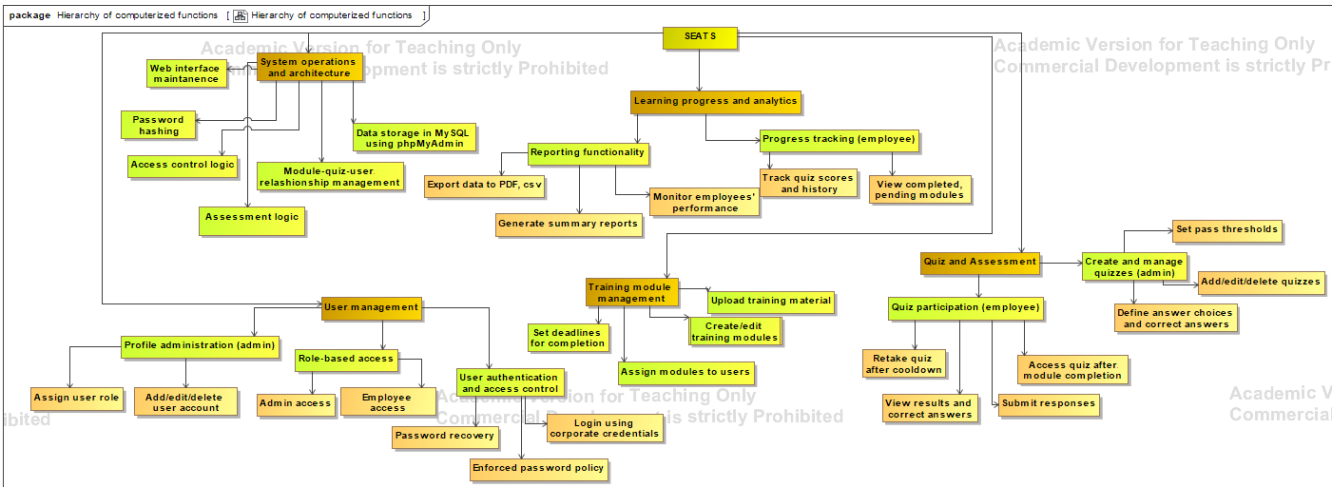
The rationale for selecting this topic is thoroughly detailed in the Introduction and Analysis sections of the report.

The purpose of developing “SEATS: Social Engineering Awareness Training System” is to swiftly establish a lightweight information system tailored for small to medium-sized organizations (0-50 employees) that offers straightforward deployment while incorporating essential functionalities and requirements pertinent to the identified topic. This system aims to educate employees about social engineering, the various types of attacks, and the diverse contextual vulnerabilities and threats specific to their field of expertise.

To serve as a proof of concept for this proposed information system, I have chosen to implement “SEATS” within a small outsourced Human Resource company, with a focus on the social engineering threats relevant to this sector. Given that HR companies handle a significant amount of Personally Identifiable Information (e.g., reviewing CVs, exchanging emails, conducting candidate assessments, etc.), employees—who represent one of the most vulnerable aspects of the organizational structure—are particularly susceptible to social engineering attacks. To mitigate the risk of data breaches, compromises of sensitive information, or system infiltrations, it is crucial for employees to recognize existing risks and to be educated on strategies to avoid them. This highlights the importance and value of this system for organizations.

4. LOGICAL STRUCTURE OF THE COMPUTERIZED SYSTEM

4.1 Hierarchy of computerized functions.



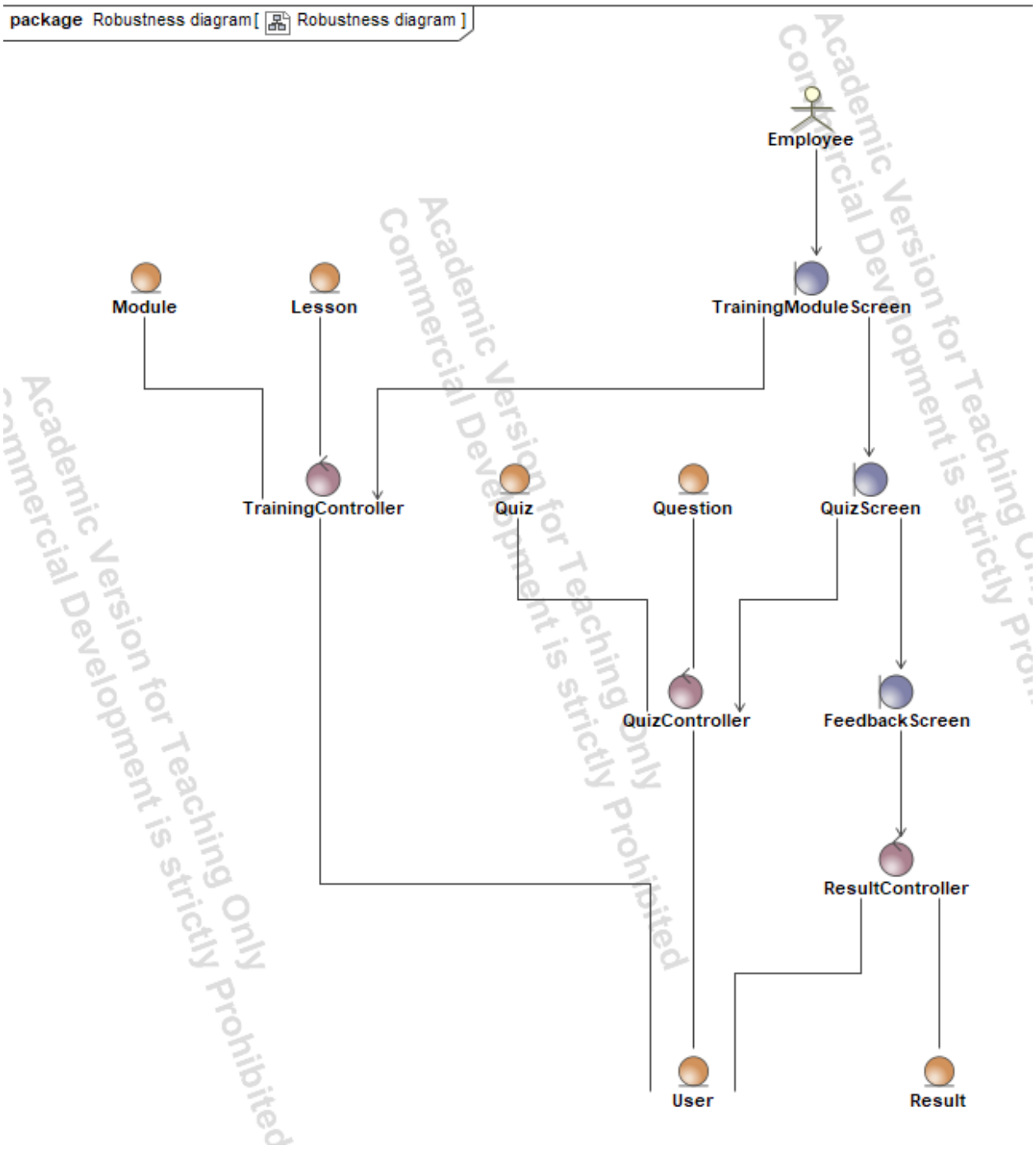
Source: created by author with the help of ChatGPT *(OpenAI, 2025)*

Figure 4 **Hierarchy of computerized functions**

This diagram outlines a hierarchy of the computerized functions, which correspond to the modules of system implementation. Main modules encompass the desired functionality, strictly covering functional and non-functional requirements, as well as business logic.

Main modules are “System operations and architecture”, “User management”, “Training module management”, “Quiz and Assessment”, “Learning progress and analytics”. They have submodules with specific functionality to be implemented.

4.2 Computerized system Robustness diagram.



Source: created by author with the help of ChatGPT (OpenAI, 2025)

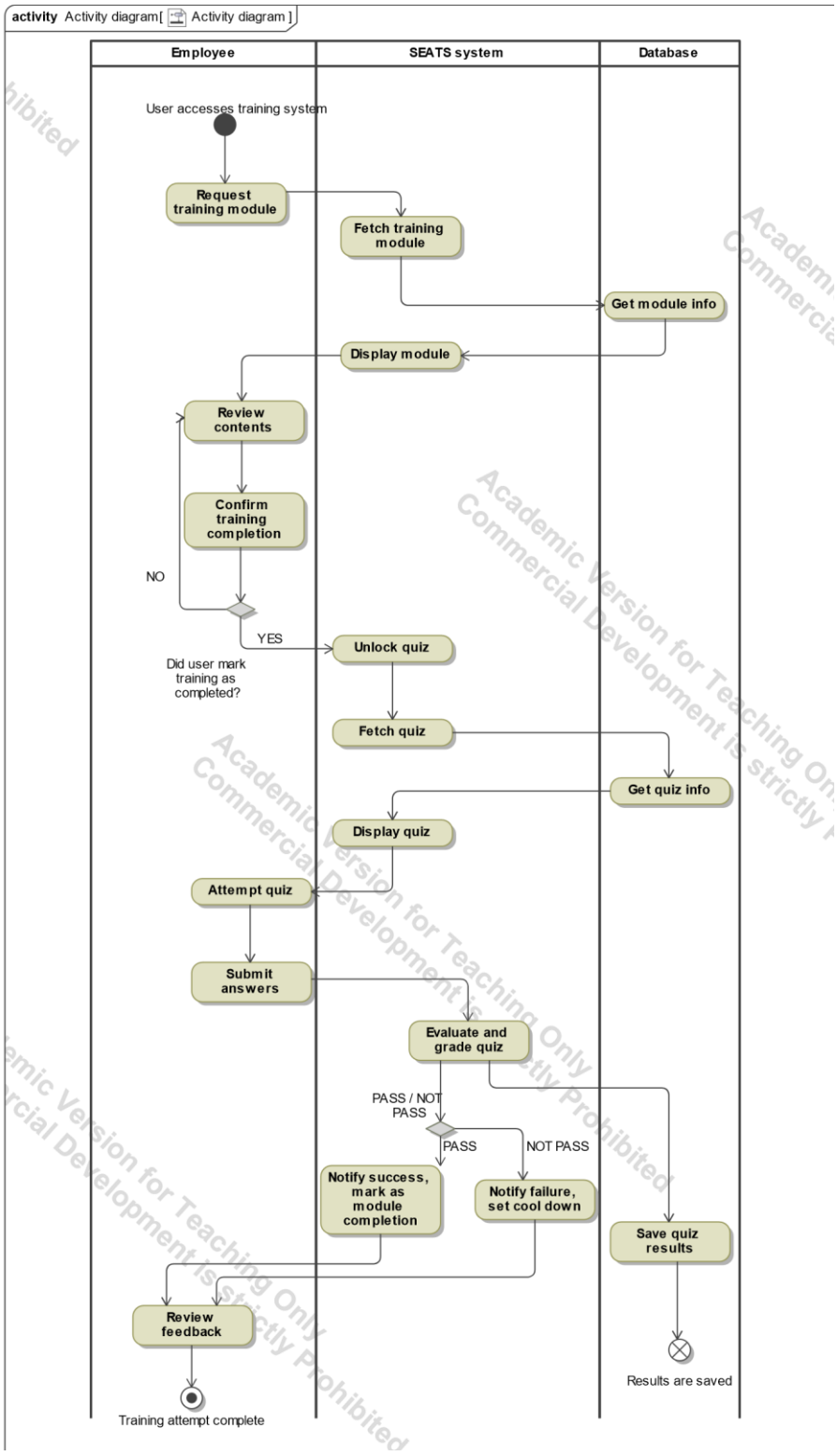
Figure 5 **Robustness diagram: Employee module training and quiz attempt flow**

Here is how module training and quiz attempt flow goes:

1. The **Employee (actor)** begins by interacting with the **TrainingModuleScreen (boundary)**, which serves as the entry point to view assigned training content.

2. The interface delegates logic to the **TrainingController (control)**, which retrieves data from:
    - 2.1 The **Module (entity)** representing the training unit
    - 2.2 The **Lesson (entity)** containing specific learning material associated with the module
    - 2.3 It also references the **User (entity)** to verify assigned modules and track completion status.
3. When lesson is completed, the **QuizScreen (boundary)** becomes active and is used to initiate the quiz attempt process.
4. The **QuizScreen** communicates with the **QuizController (control)**, which is responsible for:
    - 4.1 Retrieving the appropriate **Quiz (entity)** linked to the completed module
    - 4.2 Fetching all related **Question (entity)** items that make up the assessment
    - 4.3 Associating the submission with the correct **User (entity)** for tracking and scoring purposes
5. When the quiz is submitted, **QuizController** delegates grading and feedback responsibilities to **ResultController (control)**, which:
    - 5.1 Stores the score and evaluation details in the **Result (entity)**
    - 5.2 Links the result to the corresponding **User (entity)**
6. The processed outcome is then displayed to the employee via the **FeedbackScreen (boundary)**, completing the cycle for one training module and assessment attempt.

4.3 Computerized system Activity diagram.



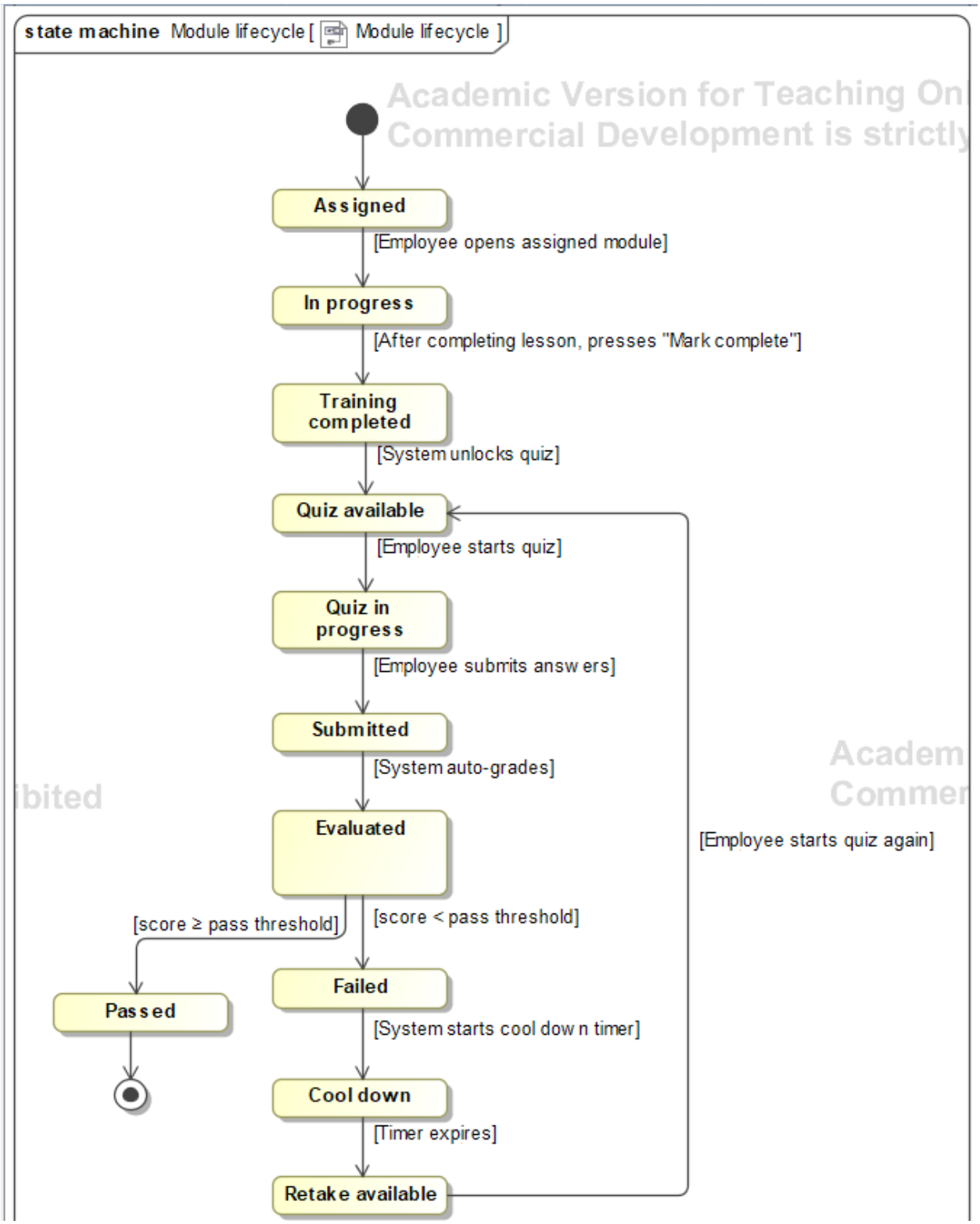
Source: created by author

Figure 6 **Activity diagram of employee attempting module completion**

This activity shows a process of employee attempting module completion. It features Employee, proposed computerized SEATS system, and Database.

Authorized employee requests and reviews the training module, marks learning complete to unlock the quiz connected to the training module. After submitting the quiz, SEATS system performs an assessment and stores the results into the Database; feedback is given to the employee and, based on the results (pass/not pass), they are notified regarding their quiz results. Data related to learning materials, quiz, and results is fetched from and stored in the Database.

4.4 System states, processes, and functioning scenario description.



Source: created by author

Figure 7 **Module Lifecycle State Machine**

This state machine diagram outlines the lifecycle of a training module assignment in SEATS. Upon assignment by an administrator, the module enters the **Assigned** state. When an employee opens it, the state transitions to **In Progress**. After the employee completes all lessons and clicks "Mark complete", the module moves to **Training completed.** The system unlocks the associated quiz and enters the **Quiz available** state. When the employee begins the quiz, it transitions to **Quiz in progress** state; upon submission, the module enters **Submitted** and then **Evaluated** states once the system auto-grades the answers. A pass threshold guard directs a successful result to the **Passed** final state. If the employee fails, the state moves to **Failed**, triggers a **Cool down** timer, and then to **Retake available**, from which the employee may restart the quiz, looping back to **Quiz in progress**. This model ensures clear enforcement of completion, assessment, and retake rules.

4.5 A formal description of calculations.

This subchapter outlines core calculation logic for SEATS. All formulas and rules were developed by author. Assistance of ChatGPT (OpenAI, 2025) was used solely to translate them into formal mathematical notation in accordance with academic guidelines.

4.5.1 Quiz scoring.

Let a quiz contain *n* questions. Each question *i* has a weight $w > 0$ (in the first deployment, weight of each question will be 1). Now we define a total weight:

$$W_{total} = \sum_{i=1}^{n} w_i = n$$

Each correct answer *s* has a weight of *w*, so the total weighted score is:

$$S = \sum_{i=1}^{n} s_i = number\ of\ correct\ answers$$

Percentage score *P* is:

$$P = \frac{S}{n} * 100\%$$

4.5.2 Pass/Fail determination.

Pass/Fail criteria is set by the administrator. Let *T* be the pass threshold, then:

$$Result = \begin{cases} Pass, & P \geq T \\ Fail, & P < T \end{cases}$$

4.5.3 Retake cool down logic.

If employee failed the quiz, they must wait a cool down *C (hours)* before retaking the quiz. Cool down is set per each failed quiz individually. System records: t(fail) = timestamp of the failure attempt. Then, earliest time to retake is:

$$t_{retake} = t_{fail} + C$$

System enforces retake:

$$AllowRetake = NOW \geq t_{retake}$$

4.5.4 Overall progress percentage.

An employee may have *M* assigned modules. Let each module *m* contribute equally to overall progress. We define:

$$ModuleScore_m = \begin{cases} 1, & LessonsComplete_m \text{^} QuizPassed_m \\ 0, & \neg(LessonsComplete_m \text{^} QuizPassed_m) \end{cases}$$

Overall progress *P* is:

$$P = \frac{1}{M}\sum_{m}^{M} ModuleScore_m * 100\% \ (0 \leq P \leq 100)$$

5. INFORMATION SYSTEM PROJECT

5.1 Input data specification.

For this part, I used the assistance of ChatGPT (OpenAI, 2025). To get correct and tailored responses, I uploaded my database project and provided this prompt: "*Based on the database project, functional requirements, and hierarchy of computerized functions, specify all input data to the system. Use tables containing fields "Component", "UI Control", "Captured field", "Validation". Prioritize main system flows and processes."*

Table 2

Quiz and question creation input data

Component	Ui control	Captured field	Validation
Quiz title	Text input	quizzes.title	1–100 chars; required
Passing threshold	Number input	quizzes.passing_threshold	0–100; default=70; required
Cooldown period (h)	Number input	quizzes.cooldown_period	≥ 0; default=1; required
Question text	Text area	questions.question_text	1–300 chars; required
Answer options (2–6)	Dynamic text inputs	answers.text	Each 1–200 chars; required
Correct option	Radio buttons	answers.is_correct	Exactly one TRUE per question

This form lets authors set up each quiz by entering its title and pass-mark, defining how soon users can retry, writing each question, listing 2–6 answer choices, and marking exactly one correct option. Fields enforce length limits (e.g. titles 1–100 chars, questions 1–300 chars, answers 1–200 chars) and require at least two choices and one correct answer.

Table 3

Module creation input data

Component	UI Control	Captured Field	Validation / Constraints
Title	Text input	modules.title	1–100 chars; required
Description	Text area	modules.description	≤500 chars; optional; strips HTML/scripts
Deadline	Date picker	modules.deadline	ISO 8601 date; ≥ today; optional
Status	Dropdown	modules.status	active | inactive; default=active; required

This form allows administrators to create new training modules by providing a title, an optional description, and an optional deadline (which cannot be set earlier than today). They can then specify the module's status as "active" or "inactive." The inputs have clear restrictions: titles can be up to 100 characters long, descriptions may contain up to 500 characters (with any HTML or scripts removed), and valid ISO-8601 dates are required, ensuring that each module is generated with complete and accurate metadata.

5.2 Output data specification.

For this part, I used the assistance of ChatGPT (OpenAI, 2025). To get correct and tailored responses, I uploaded my database project and provided this prompt: *"Based on the database project, functional requirements, and hierarchy of computerized functions, specify all input data to the system. Use tables containing fields "Component", "UI Control", "Captured field", "Validation". Prioritize main system flows and processes."*

Table 4

User progress report output data

Component	Source tables	Output field	Format / notes
User name	Users	Name	Text
Module title	Modules	Title	Text
Module status	user_module_progress	Status	Enum: not_started | in_progress | completed
Module completed date	user_module_progress	Completion_date	ISO-8601 date; blank if not completed
Overall progress (%)	Computed	–	Percent of assigned modules completed

This report surfaces each user's name with the titles of their assigned modules, showing if they have not started, are in progress, or have completed each module. For completed modules, it displays the completion date; otherwise the date field remains blank. An overall progress percentage is also calculated to give an understanding of how many modules each user has finished.

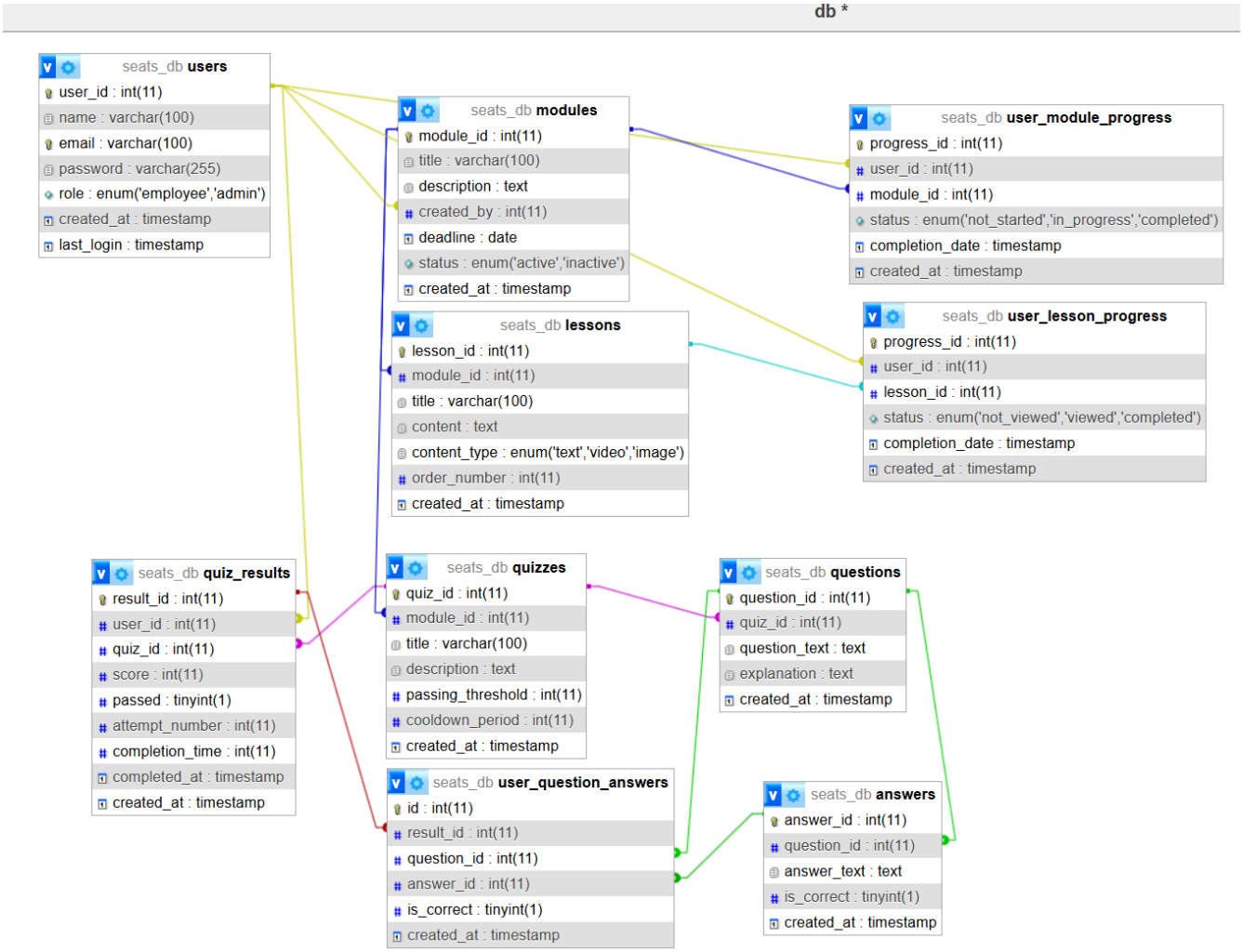
Table 5

Quiz result output data

Component	Source tables	Output field	Format / notes
User name	users	name	Text
Quiz title	quizzes	title	Text
Score (%)	quiz_results	score	Integer
Passed	quiz_results	passed	Boolean
Attempt number	quiz_results	attempt_number	Integer
Completed at	quiz_results	completed_at	ISO-8601 timestamp

his summary report lists each learner's name alongside the quiz they took, their numeric score and pass/fail status, which attempt it was, and when they completed it.

5.3 Database project



Source: created by author

Figure 8 **SEATS MySQL Database**

SEATS databased is built to encompass requirements of a simple training system and training lifecycle, from module completion and progress tracking to quiz administration and results reporting. Database schema, implemented in MySQL, organizes core entities of the system into dedicated tables: users, modules, lessons, quizzes, questions, answers, progress, results. These tables are interlinked by foreign-key relationships. The structure supports integrity and efficiency in data access and retrieval.

Table 6

Database tables description

Table	Purpose
users	Stores each user's credentials, role (employee/admin), and metadata (created, last login)
modules	Stores main information about modules: title, description, deadline, status
lessons	Stores training material, connected to module
quizzes	One quiz pre module; stores information about title, description, pass threshold and cool down period
questions	Contains questions for every quiz
answers	Stores all possible answers to questions, flags correctness
quiz_results	Records each user's quiz attempt: score, pass/fail flag, attempt number, and timestamps.
user_question_answer	Tracks which answer a user chose on each attempt
user_lesson_progress	Logs per-lesson status (not_viewed/viewed/completed) and completion date.
user_module_progress	Logs per-module status (not_started/in_progress/completed) and completion date.

REFERENCES

1 Bill Gardner and Valerie Thomas. (2014). *Building an Information Security Awareness Program.* Elsevier.

2 Anthropic. (2025). *Claude.ai*. Retrieved from Claude.ai: https://claude.ai/new

3 Bill Gardner and Valerie Thomas. (2014). Chapter 9 - Types of Training. In V. Thomas, *Building an Information Security Awareness Program* (pp. 81-88). Securicon, Lorton, VA, USA: Elsevier.

4 JGraph. (2023). *Draw.io*. Retrieved from Draw.io: https://www.drawio.com/

5 Kirvan, P. (2025, March 17). *How to avoid and prevent social engineering attacks*. Retrieved from TechTarget: https://www.techtarget.com/searchSecurity/tip/How-to-avoid-and-prevent-social-engineering-attacks

6 KnowBe4. (2025). *Security Awareness Training*. Retrieved from KnowBe4: https://www.knowbe4.com/products/security-awareness-training

7 Kron, E. (2023). *2023 PHISHING BENCHMARKING Report For North America.* KnowBe4. Retrieved from https://www.knowbe4.com/hubfs/2023-Phishing-Benchmarking-Results-For-North-America-Guide_EN.pdf?hsLang=en-us

8 OpenAI. (2025). *OpenAI*. Retrieved from ChatGPT: https://chatgpt.com/

9 proofpoint. (2024). *2024 State of Phish \ Report.* Retrieved from proofpoint.: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf

10 proofpoint. (2024, November). *Proofpoint ZenGuide.* Retrieved from proofpoint.: https://www.proofpoint.com/sites/default/files/solution-briefs/pfpt-us-sb-zenguide.pdf

11 proofpoint. (2025). *Mitigate Human Risk.* Retrieved from proofpoint.: https://www.proofpoint.com/us/products/mitigate-human-risk

12 Sveidqvist, K. (2025). *Mermaid Chart*. Retrieved from Mermaid: https://www.mermaidchart.com/

13 Walter Fuertes, Diana Arévalo, Joyce Denisse Castro, Mario Ron,Carlos Andrés Estrada, Roberto Andrade, Felix Fernández Peña,and Eduardo Benavides. (2021). Chapter 3. Impact of Social Engineering Attacks:A Literature Review. In *Developments and Advances in Defense and Security* (pp. 25-35). Springer.