University of Bahrain
College of Information Technology
Department of Information Systems
B.Sc. In Cyber security

A Behavior-Oriented Web-Based Cybersecurity Awareness and Assessment System for Organizations (Corporate CyberAware)

Prepared by:

Anfal Isa Alsowaileh - 202207510
Dana Yusuf Alsendi - 202207869
Duha Zuhair Isa - 202206159

For
ITCY499
Senior Project
Academic Year 2025-2026-Semester 2
Project Supervisor:
Dr. Yaqoob Salman Mohamed Alslais
Date of Submission

Abstract

In the world of technology, cybersecurity incidents have become increasingly prevalent and are often driven by human behavior rather than just technical failure. Our project aims to address this issue by introducing Corporate CyberAware, a behavior-oriented web-based system designed to elevate how companies deal with employees' cybersecurity awareness. In traditional programs, they often rely on one-time training and do not really measure user behavior, leaving companies weak and open for threats like phishing and bad security practices. In order to close this gap, our project provides continuous assessments, tracking user performance, and phishing simulations to keep track of and evaluate employee behavior over time. Our system strives to offer an adaptive and interactive learning environment and shift cybersecurity awareness from static to continuous and behavioral, enabling companies to reduce human-related cybersecurity risks.

Acknowledgment

The completion of our project would never have been possible without the teamwork, guidance, and experience that contributed to the development of this project. A huge thanks goes to Dr. Yaqoob Salman Mohamed Alslais for his great guidance and contribution throughout the entirety of this project; his support and valuable feedback were extraordinary for us during the course. The quality and direction of our work were heavily influenced by his dedication, expertise, and great work ethics.

We would like to extend our appreciation to the College of Information and Technology at the University of Bahrain for facilitating a smooth workflow and the required academic environment to perform this project.

A special thanks goes to our families and friends for their patience, encouragement, and continuous support throughout the development of this project. Their constant motivation was the most necessary in completing this project successfully.

Table of Contents

Chapter 1: Introduction

1.0 Problem Statement

A growing number of security incidents are being reported in organizations, most of which are caused by human behavior rather than technical flaws. Employees may unknowingly expose systems to security risks by clicking on phishing links, using weak passwords, or not adhering to security policies.

In recent years, cyber threats have increased significantly in Bahrain. An estimated 735,244 phishing attacks were reported in 2022, demonstrating the increasing impact of social engineering attacks on organizations. Moreover, the National Cyber Security Centre (NCSC) reported that 80.95% of vulnerabilities require user interaction, confirming that human behavior plays a major role in cybersecurity.

There are a number of challenges organizations face when it comes to cybersecurity awareness programs:

- Lack of continuous assessment: The majority of awareness programs are conducted as one-time training with no ongoing evaluation.
- Limited focus on behavior: The majority of existing approaches are focused primarily on knowledge.
- Lack of performance tracking: Corporations lack the tools necessary to track employee progress and identify areas for improvement.

Consequently, current awareness programs do not sufficiently ensure long-term improvements in cybersecurity behavior. To reduce human-related cybersecurity risks, organizations require a system that monitors and continuously evaluates employee awareness, tracks performance, and helps reduce the risk of human error.

1.1 Project Objectives

The primary objective of this project is to design and develop a web-based system that will enhance cybersecurity awareness among employees in organizations. This project has the following objectives:

- Develop a system for assessing common risks.
- Assess employee performance based on their responses and behavior.

- Track employee awareness and performance.
- Support continuous assessment of cybersecurity awareness.

Scope:

The system is intended for use by employees and administrators within organizations. The web-based platform includes cybersecurity awareness, assessment, and performance tracking.

Limitations:

System capabilities do not include real-time detection of attacks or advanced security protection. The focus is solely on improving the awareness and behavior of users within an organization.

1.2 Relevance/Significance of the project

The importance of this project lies in the fact that it addresses the human factor in cybersecurity, which is a major cause of security incidents. This project has the following significance:

- Provides a behavior-based approach to cybersecurity awareness rather than focusing only on theoretical concepts.
- Enhances continuous assessment rather than one-time training.
- Enhances employee cybersecurity practices by identifying weak areas.
- Tracks the performance of employees over time.
- Provides an integrated web-based platform for assessment and monitoring.

1.3 Report Outline

The report is structured in the following manner. An abstract provides a brief overview of the project, followed by a section of acknowledgement. In chapter 1, the project is introduced, and the problem statement and objectives are presented. In Chapter 2, the literature review relating to cybersecurity awareness and human behavior is presented. In Chapter 3, a description of the approach and methodology used to manage the project is provided. In Chapter 4, requirements collection and system analysis are discussed. As part of Chapter 5, the system design is presented, including the database, user interface, and algorithms. In Chapter 6, we discuss the implementation and testing of the system. Last but not least, Chapter 7 concludes and discusses future directions.

Chapter 2: Literature Review

2.0 Introduction

Cybersecurity incidents in organizations are commonly caused by human behavior (Ussher-Eke, 2025). Employees may be exposed to cyber threats by responding to phishing emails, using weak passwords, and not following security policies. The Daily Tribune - News of Bahrain reported an increase in cyberattacks, including thousands of phishing attempts, which reflects the increasing severity of user-targeted attacks (The Daily Tribune - News Of Bahrain, 2022). Furthermore, the National Cyber Security Center emphasizes that many vulnerabilities are a result of user interaction, which highlights the critical role that employees can play in helping to mitigate security incidents (National Cyber Security Center, n.d.).

It is clear from these issues that organizations need structured and continuous cybersecurity awareness solutions. Consequently, a web-based system that assesses employee awareness and promotes secure behavior is essential for reducing human-related cyber risks.

The aim of this literature review is to examine the role human behavior plays in cybersecurity incidents and the importance of cybersecurity awareness in organizations. It reviews existing awareness programs and points out their limitations, particularly the lack of continuous assessment. As part of the review, we also examined the effectiveness of current cybersecurity awareness and training frameworks in improving users' behavior. Additionally, it discusses the methodologies for assessing awareness levels as well as the reliability of these methods. As a final section, it discusses advanced techniques, such as gamification and simulation, highlighting their advantages and disadvantages. The results of this study can be used to identify gaps and to support the need for a behavior-oriented cybersecurity awareness and assessment system.

2.1 Human Behavior as a Primary Cause of Cybersecurity Incidents

In professional life, human behavior has been recognized as the primary contributor to cybersecurity incidents. Research consistently suggests that user action is what creates vulnerabilities and opens the door to cybersecurity attacks that technical controls alone cannot prevent, as well as influencing decision-making and cognitive bias. According to (Quchi, et al., 2024), despite having substantial technological improvements and advancements, the human factor is still the main persistent reason for security breaches, mainly due to ineffective awareness, cognitive overload, and security fatigue. The study points out that even with robust and strong technical measures, staff interactions with digital systems, such as skipping security protocols or misusing passwords, can compromise company security. It also implies that to enhance overall resilience and endurance, cybersecurity initiatives must incorporate a human-centered approach that integrates behavioral understanding into system design, training, and evaluation procedures.

Furthermore, (Pothu, 2025) explores the user behavior and the role it plays in allowing cyber threats, displaying that having weak password practices, phishing attacks, and low risk perception are usually motivated by users' limited awareness of cyber risks and convenient decisions. The study illustrates that human behavior can have a direct effect on the success of cyberattacks by revealing that those with minimal cybersecurity awareness are much more likely to fall for phishing and social engineering attacks. Additionally, the study suggests that merging behavioral analysis alongside cybersecurity strategies will enable organizations to design cybersecurity awareness and training programs that address and target specific weaknesses in users. This study proves to us once again that understanding the behavioral habits of users is mandatory to develop effective and efficient preventative measures and enhance the cybersecurity posture of organizations.

Moreover, the study (Donekal Chandrashekar, et al., 2024) highlights that cybersecurity is not only about the technical controls and inventions but also a human behavioral one, pointing out that the decisions the users make during cyber incidents are what determine if the threat will escalate or be controlled. The analysis in this research showcased that following the traditional manners in security defenses will tend to fail to grasp the complexity of human decision-making in evolving attack scenarios and demands systems that are capable of continuously observing and evaluating user behavior. The research emphasizes the significance of gathering behavioral data to strengthen the training and system design and suggests the need for immersive and simulation-based methods to understand user responses during cyberattacks. The importance of incorporating behavioral knowledge into cybersecurity solutions, especially in organizational settings where user behavior strongly influences security outcomes.

All in all, these papers prove that human behavior is the main reason for cybersecurity incidents and that awareness programs and technical controls are not enough for successful protection. The recurring feedback and recommendations in literature are implementing a behavior-focused and continuous cybersecurity awareness training instead of having one-time sessions, as well as integrating analysis strategies on behavior to understand user weaknesses. Also, the studies delve into the importance of providing ongoing feedback for users to make sure that secure practices are enforced and to add to the long-term behavioral change. In our project, we propose a behavior-oriented approach that continuously evaluates behavior, provides targeted training accordingly, and develops a design that is user-centered.

2.2 Cybersecurity Awareness in Organizational Contexts

The concept of cybersecurity awareness has become an essential component in organizational security measures, since employees' knowledge, attitudes, and behaviors can drastically influence the success of technical and operational strategies. According to recent studies, corporates are realizing the importance of cybersecurity awareness and the role it plays in reducing human-related vulnerabilities and enhancing security culture. (Ünsal & Ocak, 2026)

Showcased that organizational policies, regulatory knowledge, and technical controls are all part of cybersecurity awareness in addition to individual knowledge. The study presents the Organizational Cybersecurity Awareness Scale (OCAS), which is an established framework that is designed to measure the scale of awareness across multiple domains inside public-sector organizations. According to the authors, many companies lack dependable methods to properly evaluate awareness levels, which makes it difficult to identify the weaknesses or assess the effectiveness of training. The study emphasizes the value of providing structured evaluation techniques that can enhance focused training and organizational decision-making by underlining the necessity of systematic and validated awareness measurements.

Moreover, (Shouq Alrobaian, 2023) provides empirical evidence of gaps in awareness among users in organizations, showing that poor cybersecurity awareness plays a major role in unsafe behaviors and policy compromises. According to the study that surveyed 739 individuals in an organization, a large portion of respondents (68.6%) had never taken part in any kind of formal awareness training, and only 31.4% of the participants had ever attended a cybersecurity awareness program. Interestingly enough, a serious absence in previous association with cybersecurity practices was demonstrated by the fact that 64.1% of participants admitted that this was the first time they had ever discussed cybersecurity issues connected to the devices they usually use. The study revealed a noticeable lack of technical and behavioral awareness, where 40.87% reported they lacked antivirus protection. The good news is that the majority (68.5%) believed that cybersecurity awareness programs are essential for preventing cyberattacks, showing that there is recognition for cybersecurity awareness. These findings illustrate the importance of having continuous awareness training and behavioral guidance within organizational contexts.

(Taherdoost, 2024) adds that successful cybersecurity awareness in organizations demands adaptive and integrated training methods that are capable of improving employee engagement and knowledge absorption. In order to improve training outcomes, the study proposes the Integrated Cybersecurity Awareness Training (ICAT) model, which blends gamification, microlearning, and real-time monitoring. The study reveals that organizational cybersecurity awareness must be viewed as a continuous process instead of a one-time solution by promoting continuous, interactive, and measurable training approaches. The findings underline the need for systems to integrate training with monitoring and assessments to ensure long-term improvements in employee awareness behavior.

These studies have shown that organizations need cybersecurity awareness to be viewed as multidimensional and continuous processes, requiring reliable assessment methods and proper integration with organizational policies and practices.

2.3 Limitations of Traditional Cybersecurity Awareness Programs

Regardless of the prevalent adoption of cybersecurity awareness strategies, many existing programs remain limited in their effectiveness and viability. A common feature of such initiatives is that they are intended to be compliance-driven and delivered as one-time activities, where employees participate mainly to comply with the regulatory requirements. In such cases, training and assessments are performed as obligations rather than as a sustainable, continuous educational process, which curtails employee engagement and motivation. According to (Ussher-Eke, 2025), compliance-driven awareness campaigns often fail to achieve behavioral changes, as users discern assessments as administrative tasks rather than security tools.

Another major limitation of current programs is the dependence on universal awareness content, unassertive learning techniques, and frequent adoption of standard learning materials, including slides, videos, or short knowledge checks, collectively disregarding employees' roles or professions. Latest literature accentuates that unified approaches lack pertinence and applicability, deterring employees' ability to apply acquired knowledge to real-world practices (Ussher-Eke, 2025).

Furthermore, current awareness programs manifest the lack of behavioral focus. Although they aim to foster awareness and increase knowledge, they neglect considering the psychological aspects that influence security decision-making. Studies acknowledge that cybersecurity risk is influenced primarily by self-efficacy, risk anticipation, and individual perspectives (Bishop, et al., 2025). Similarly, the CAT frameworks recognize that human behavior and practices constitute the predominant cause of vulnerability (Hijji & Alam, 2022).

Comprehensively, current cybersecurity awareness programs are considered limited by their compliance-driven, dormant, and generic essence, requiring the need for adaptive and behavior-focused techniques.

2.4 Cybersecurity Awareness and Training Frameworks

In response to the drawbacks of existing awareness strategies, multiple cybersecurity awareness and training frameworks have been developed to enhance organizational security behaviors and practices. These frameworks seek to structure awareness efforts by incorporating assessment, training, and enrichment mechanisms into standard models. In contrast with conventional programs, framework-based approaches strive to align employee awareness growth with corporate cybersecurity objectives.

Remarkable examples include the Cybersecurity Awareness and Training (CAT) Framework (Hijji & Alam, 2022), the Employee Cybersecurity Awareness Framework (Bishop, et al., 2025), and the Integrated Cybersecurity Awareness Training model (ICAT) (Taherdoost, 2024). Overall, these frameworks reinforce systematic assessments, user-centric design, and perpetual

learning as core features of effective awareness systems. However, although these frameworks have provided significant advancements, they also inherit practical constraints that limit their effectiveness in real corporate environments.

2.4.1 Cybersecurity Awareness and Training (CAT) Framework

The CAT framework discussed in (Hijji & Alam, 2022) establishes a strong model by structuring it into three hierarchical levels based on cognitive depth and maturity—awareness level (beginner), training level (medium), and assessment level (advanced) and twenty-five core behavioral practices constructed mainly to measure employee cybersecurity knowledge and provide training guidance. A core feature of the CAT framework is the maturity-based approach, where users are categorized according to examined capability levels and performed practices.

Despite its systematic nature, the CAT framework remains static and knowledge-focused, as it fails to adapt to evolving threat environments or changing user practices, which directly limits its sustained effectiveness regardless of identifying knowledge deficits.

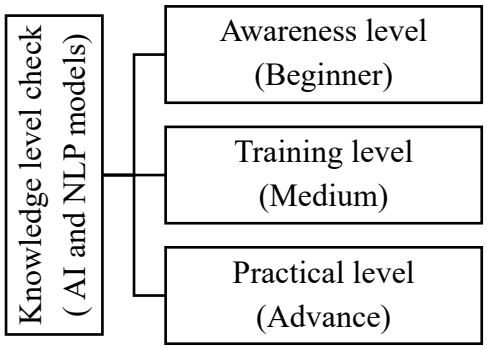

Figure 2.1 Cybersecurity Awareness and Training (CAT) Framework (Hijji & Alam, 2022)

2.4.2 Employee-Centered Awareness Frameworks

Specialized employee-centered models emphasize behavior-associated risks rather than knowledge delivery. Recent studies, including (Bishop, et al., 2025), have analyzed psychological factors causing vulnerabilities, demonstrating that cybersecurity awareness contributes to over 55% of risk behavior disparities.

The ECAF introduces six core dimensions to provide comprehensive risk assessment and focused behavioral and psychological profiling beyond knowledge assessments. Dimensions include threat appraisal, self-efficacy, awareness, security attitude, operation policy, and cybersecurity experience and involvement as identified by (Bishop, et al., 2025)

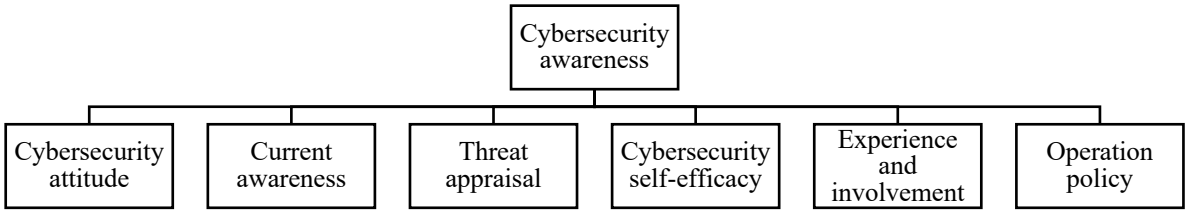

Figure 2.2 Employee Cybersecurity Awareness framework (ECAF) (Bishop, et al., 2025)

Similarly, ICAT consolidates emerging technologies such as gamification, micro-learning, and adaptive feedback into a holistic framework to deliver targeted training, enhance engagement, and improve knowledge retention (Taherdoost, 2024).

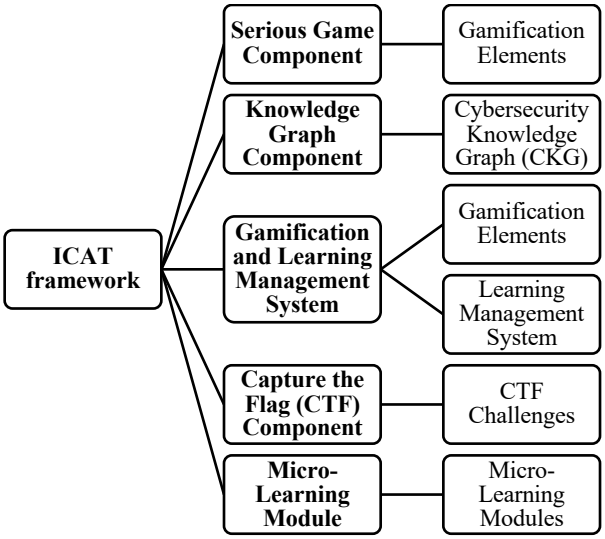

Figure 2.32 Integrated Cybersecurity Awareness and Training (ICAT) Framework (Taherdoost, 2024)

Nevertheless, discussed frameworks provide meaningful theoretical rationale, while practical malleability and real-time functionality remain limited due to reliance on self-assessment data and conceptuality lacking full system-level synthesis.

These constraints mandate the need for adaptive and behavior-focused cybersecurity awareness systems in corporate environments.

2.5 Assessment and Measurement of Cybersecurity Awareness

It is important to assess cybersecurity awareness as part of organizational security management, as it helps determine whether users are truly aware of safe practices, rather than only receiving theoretical training. The lack of proper measurement can limit awareness programs. It is critical that organizations conduct regular assessments to identify knowledge gaps. Moreover, they should monitor their employees' risky behaviors and develop customized measures to reduce specific vulnerabilities in their security systems.

Surveys and questionnaires offer structured and quantitative data on users' knowledge, attitudes, and security practices, which helps measure their awareness levels. The use of these tools allows organizations to evaluate overall awareness, compare group results, and identify areas that need improvement. These approaches allow feedback to be collected efficiently from large groups (Shouq Alrobaian, 2023).

However, surveys and questionnaires do not always reflect the real security behavior of employees. Employees may overestimate their knowledge or choose answers that they believe are correct rather than describe their actual practices. As a result, awareness levels measured through self-reports can sometimes be inaccurate. The best way to find out if security policies are being followed is to watch what people do, such as password management, how they respond to phishing attempts, and how well they follow security rules. You need to look at how employees act in real life, not just at what they say. Therefore, combining surveys with behavioral assessments gives a more reliable and accurate measure of cybersecurity awareness (Pothu, 2025).

2.6 Advanced Awareness Techniques: Gamification and Simulation

Simulations and gamification are modern advancements over traditional training methods, which tend to be passive and relatively ineffective (Ussher-Eke, 2025). These techniques rely on interactive activities and realistic scenarios to involve users. Gamification motivates participation by using quizzes, challenges, and rewards to improve engagement (Shaik Mohammed Junaid, 2025). Simulation-based training programs can provide users with the opportunity to experience realistic cyber threats in a controlled environment, such as phishing attacks, where they can learn how to avoid them.

Gamified and Simulation-Based approaches have been shown to be effective in improving user engagement and knowledge retention (Ussher-Eke, 2025). Through interactive training, participants are involved in the learning process and are exposed to cybersecurity concepts repeatedly, which reinforces correct cybersecurity behavior. A scenario-based simulation enhances the users' ability to recognize and respond to threats in real-world situations. Consequently, these methods encourage users to demonstrate better awareness and stronger retention compared to traditional awareness training (Ussher-Eke, 2025).

While these improvements have been made, gamification and simulation are still lacking continuous assessment. Often, these techniques are applied in periodic training sessions, which provide only a short-term assessment of user awareness. In the absence of ongoing monitoring, adaptive feedback, and long-term measurement of user behavior, improvements in engagement and retention may decline over time (Ussher-Eke, 2025). Although gamified and simulated training represents an important advancement in cybersecurity awareness, their effectiveness remains limited without continuous assessment mechanisms (Ussher-Eke, 2025).

2.7 Comparison with Existing Framework

After reviewing the increasing literature regarding human behavior as the primary factor in cybersecurity attacks, there has been a noticeable gap between having awareness-focused frameworks and systems that properly transform cybersecurity awareness into a continuous, sustainable, and secure behavior in the context of an organization. Current research and frameworks heavily concentrate on static assessments and knowledge sharing, often relying on self-reported questionnaires and general information that fail to capture real behavioral responses to emerging threats (Hijji & Alam, 2022) (Taherdoost, 2024). Latest studies affirm the impact and efficacy of simulations, gamification, and adaptive learning in strengthening engagement, but such methods are commonly utilized and implemented as standalone training tools rather than as continuous assessments (Saif Al-Dean Qawasme, 2025) (Ussher-Eke, 2025). In other words, studies show that there is a lack of cohesive, integrated, web-based platforms that amalgamate behavior-focused assessment, continuous monitoring, and customized feedback that is specific to organizational roles, indicating significant research and practical lack that this project seeks to improve.

Table 2.1 compares core aspects including focus, assessment type, behavioral monitoring, customization, and feedback mechanism. Focus refers to the framework's main objective and concentration, whether it examines knowledge, analyzes psychological behavior, or is a continuous learning and assessment process. Assessment type defines how users' awareness is measured, such as generic questionnaires, surveys, or selected assessments chosen by the administrator. Behavioral monitoring specifies whether the framework is tracking user actions or considering self-reported responses. Customization refers to whether assessments are generic or specifically assigned to users. Finally, the feedback mechanism describes how users receive guidance and training recommendations.

Feature / Aspect	**CAT** (Hijji & Alam, 2022)	**ECAF** (Bishop, et al., 2025)	**ICAT** (Taherdoost, 2024)	**Proposed System**
Focus	Knowledge maturity levels	Behavioral dimensions	Adaptive learning	**Continuous behavior assessment and enhancement**
Assessment Type	Questionnaires	Surveys	Frequent evaluations	**Customized assessments**
Behavioral Monitoring	No	Limited (psychological)	Yes	**Yes (performance based)**

Customization	Generic	Profiling	Partial	**Personalized**
Feedback Mechanism	Limited	Conceptual (theoretical)	Adaptive feedback	**Real-time**

Table 2.1 Comparative analysis between discussed cybersecurity awareness frameworks and the proposed system

2.8 Solution

Based on current literature and existing frameworks such as CAT (Hijji & Alam, 2022) and ECAF (Bishop, et al., 2025), this study propounds a platform for corporate environments that measures cybersecurity awareness by offering administrator-driven assessments. Unlike existing approaches that emphasize questionnaires and generic training materials, this study coordinates continuous assessments and result-driven observations to specify awareness deficiencies and generate targeted training requirements. The proposed system combines assessment, customization, and feedback within a single platform to align the gap between theoretical awareness frameworks and practical organizational needs, improving both employee cybersecurity practices and the organization's overall security level.

Chapter 3: Project Management

3.0 Process Model (SDLC Model)

For a project, the Software Development Life Cycle (SDLC) is crucial for developing and delivering a high-quality software system. SDLC is a framework that is used to structure the processes of planning, developing, designing, and testing a system (Hossain, 2023). In our project, we found that the Agile model is the best fit. It is an iterative methodology that works in increments, where you work in small cycles and produce a version of your work on the system (Hossain, 2023). Figure 3.1 displays the iterative development cycle from the Agile process model, the cycle consists of planning the iteration goals and requirements, designing the system's architecture and interfaces, developing the code of the website and modules, testing each unit and its integration, and evaluating every iteration and feedback. This model gave us the ability to evaluate and improve our work continuously.

A lot of reasons made us choose the Agile model; since it is a web-based system, it will always require continuous enhancements and adjustments. Also, our project consists of multiple components like the user, admin, and training, and they each require gradual development. Agile provides the flexibility of modifying and adding features, especially with testing and the supervisor's feedback.

The project applied Agile by dividing the processes of development into iterations. First, the requirement analysis, where we identify main features like users' assessments and report generations. Second, the design phase is planning the system structure and architecture of the web system as well as the user interfaces. Then, the implementation phase is planned to develop the system modules incrementally, where the user login is developed first, followed by the assessment, administrator, and reporting functions. The process of small to big makes sure that each module is properly functioning.

Moving on, the testing phase attempts to test each module individually after finishing development to make sure it is accurately working. Lastly, the evaluation phase is where we review the system and its performance based on feedback and testing results. Overall, choosing the Agile model gave us the flexibility and proper structure to be able to develop our project in an efficient and improvable manner.

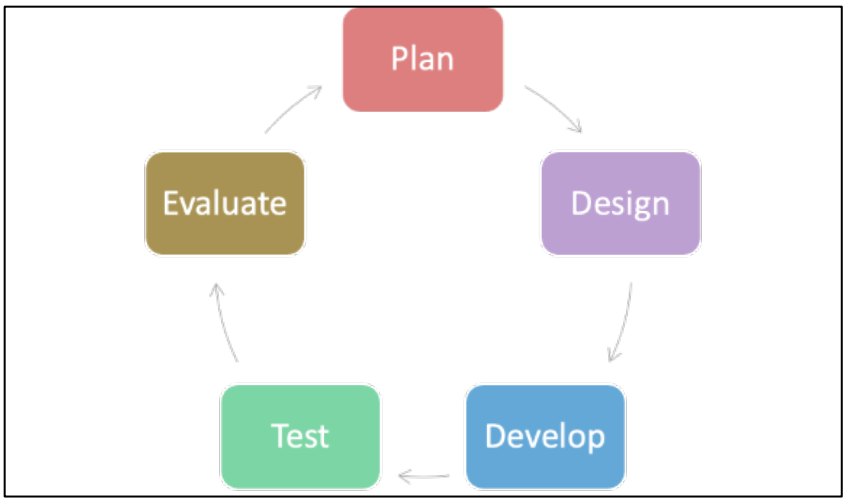

Figure 3.1 Agile Iterative Cycle

3.1 Risk Management

Risk management is a mandated part of the project plan and includes identifying technical and organizational risks, analyzing their reflective effect on project delivery,
and establishing appropriate mitigation strategies to reduce their impact. This approach ensures that risks and their impacts are managed efficiently through strategic planning and continuous monitoring. Accordingly, the project is expected to be delivered successfully on time and meet the specified functional requirements.

The proposed system is considered a relatively low-risk project due to the use of emerging technologies and its corporate applicability scope. Based on this, project risk management emphasizes early identification of risks and planning mitigation strategies to minimize their impact on the project's completion. Nevertheless, multiple technical and organizational risks were recognized, including the lack of technical knowledge, unavailability of team members, development delays, system bugs or errors, and possible system requirements changes.

The majority of identified risks are categorized as medium-level risks and considered manageable through appropriate task distribution and regular meetings. High risks such as system bugs and errors are mitigated through compliance with software development lifecycle (SDLC) practices and continuous testing.

ID	Risk Description	Probability	Impact	Mitigation Plan
RM1	Team member unavailability	Medium	Medium	Learn required technologies through online tutorials
RM2	Lack of technical knowledge or experiment in certain technologies and programming languages affecting project competence and quality	Medium	High	Ensure all members understand system components and share tasks according to the activity plan
RM3	Development delays affecting deliverable submissions due to resource constraints and inappropriate time management	Medium	Medium	Establish a clear project schedule and track progress by reviewing weekly milestones
RM4	System bugs or errors increase during development, affecting system robustness and reliability	High	High	Test system frequently and fix errors immediately
RM5	Requirement changes and modifications necessitating system redesign and additional testing	Low	Low / Medium	Follow the Agile model to handle and adjust changed system requirements

Table 3.1 Identified project risks and mitigation strategies

3.2 Project Activities Plan

This project's activities plan outlines the structure of the proposed Behavior-Oriented Web-Based Cybersecurity Awareness and Assessment System for Organizations over several academic weeks. In this project, a phased and incremental approach is utilized, beginning with the analysis of requirements and culminating with the delivery and presentation of the system. A Gantt chart is used to visualize the task dependencies and durations during the project. By following this structured planning process, academic deadlines are met, time is effectively managed, plans are scheduled, and the academic program is executed in a timely manner.

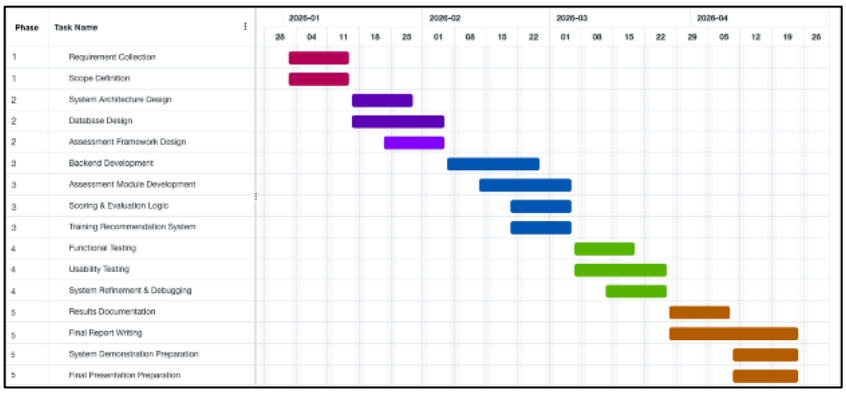

Figure 3.2 Gantt Chart of the Project Activities Plan

Figure 3.2 illustrates the project's progress from planning and designing to implementing, testing, and delivering. Certain activities overlap to ensure efficient time management. The overlap between implementation and testing activities is indicative of the iterative development approach, which enables early identification of issues and continuous system improvements.

Phase 1 (Weeks 1-2) Planning: This phase focuses on collecting requirements and defining the project scope. It identifies system requirements, user roles, and cybersecurity risk factors to establish a clear framework.

Phase 2 (Weeks 3-5) Design: This phase is dedicated to system design. It includes defining the system architecture, database structure, and assessment framework to prepare for implementation.

Phase 3 (Weeks 6-9) Implementation: This phase focuses on implementing the system and core development activities. The backend, assessment module, scoring logic, and recommendation system are developed and integrated during this phase.

Phase 4 (Weeks 10-12) Testing: The main objective of this phase is system testing and evaluation. Functional and usability testing are conducted to verify performance and refine system components.

Phase 5 (Weeks 13-16) Delivery: The final phase involves report completion and overall project delivery. Results are documented, the system is demonstrated, and the final presentation is prepared.

Chapter 4: Requirement Collection and Analysis

4.0 Introduction:

This chapter presents the requirements of collection and analysis for the proposed behavior-based cybersecurity awareness system, Corporate CyberAware. This chapter focuses on determining the system requirements from collected data, taking into consideration both functional and non-functional aspects, and introducing system models to provide a clear understanding of how the system is designed and operated.

4.1 Requirement Elicitation

We collected the system requirements by utilizing a survey, which included 18 questions and received 110 responses. The survey evaluated cybersecurity knowledge, practices, training, and the need for continuous assessment and tracking systems. As a result of the survey, gaps in current cybersecurity practices have been identified, and cybersecurity awareness needs to be improved.

In Figure 4.1, the majority of respondents are between the ages of 35 and 44, followed by those aged 18 to 24 and those between 25 and 34. Clearly, there was a wide range of ages represented in the survey.

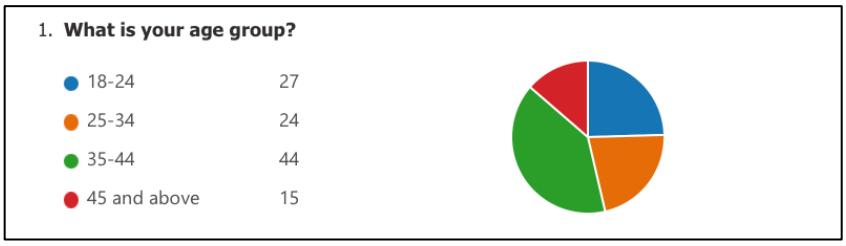

Figure 4.1: Age Group Distribution of Respondents

Figure 4.2 shows that most respondents are females (65%), while the percentage of male respondents is 35%. The survey showed a higher participation rate among female respondents.

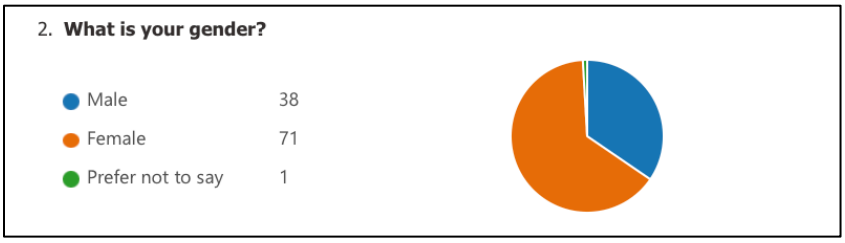

Figure 4.2: Gender Distribution of Respondents

According to Figure 4.3, most respondents have a bachelor's degree (70%), followed by a postgraduate degree (14%). Based on these results, the survey responses are considered reliable due to most respondents having a high level of educational background.

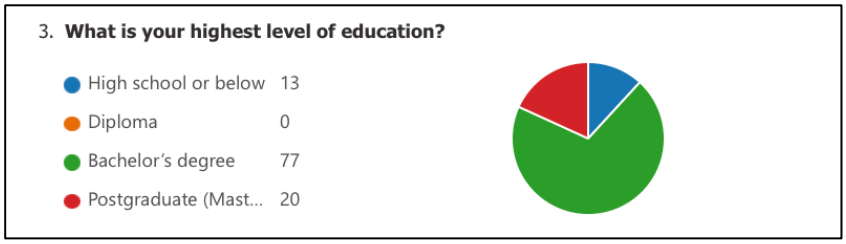

Figure 4.3: Respondents' Highest Level of Education

Based on 4.4, most respondents are employees (58%), followed by IT professionals. As a result, it appears most of the survey's results are based on perspectives from working professionals, which are aligned with the security requirements of organizations.

Figure 4.4: Distribution of respondents based on their role

In Figure 4.5, a significant percentage of respondents have not received cybersecurity awareness training or have received it only occasionally. Specifically, 30% (33 respondents) have never received training, while 25% (28 respondents) received it occasionally and 19% (21 respondents) only once. Only 25% (28 respondents) reported receiving training regularly. This illustrates the lack of a consistent approach to cybersecurity awareness training in organizations.

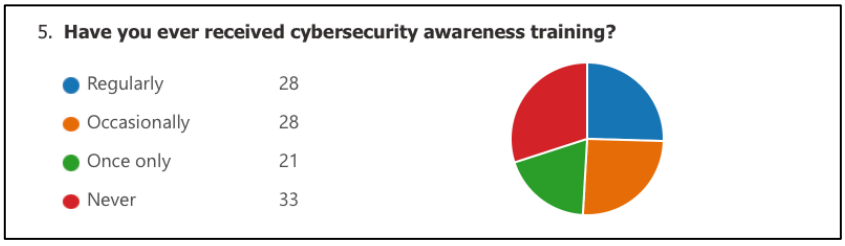

Figure 4.5: Responses to cybersecurity awareness training

Figure 4.6 shows that the majority of respondents rated their cybersecurity knowledge as low or moderate. Specifically, 38% rated their knowledge as moderate, 36% as low, 16% as high, and 9% as very low. This indicates that participants do not have a very high level of cybersecurity awareness.

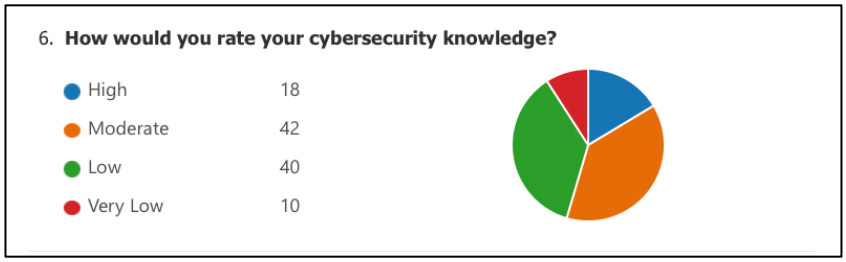

Figure 4.6: Respondents' level of cybersecurity knowledge

Figure 4.7 indicates that cybersecurity training is not consistently provided. Specifically, 35 respondents stated that training is provided sometimes, 30 respondents frequently, 25 respondents rarely, and 20 respondents never. This shows that organizations do not regularly implement cybersecurity training.

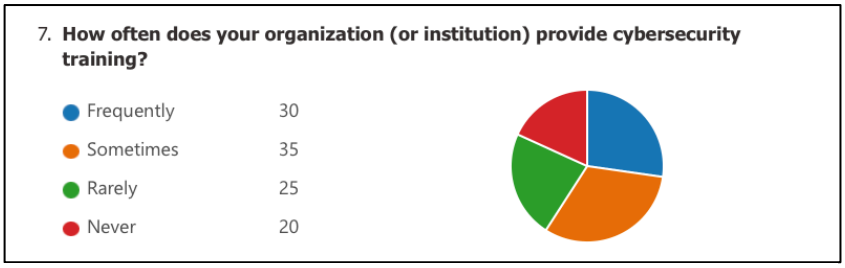

Figure 4.7: Frequency of Cybersecurity Training in Organizations

In Figure 4.8, most respondents are confident or somewhat confident in identifying cybersecurity threats. Specifically, 39% are confident, 25% are slightly confident, 20% are very confident, and 15% are not confident. This indicates that while some awareness exists, improvement is still needed.

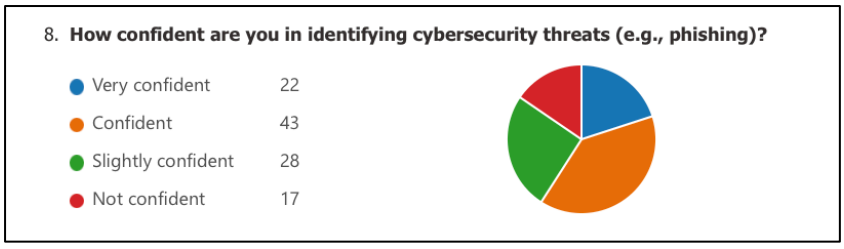

Figure 4.8: Confidence in Identifying Cybersecurity Threats

Based on Figure 4.9, a significant percentage of respondents reuse the same password on a regular or occasional basis. Specifically, 38% reuse passwords often, 33% sometimes, 23% always, and only 6% never reuse passwords. This indicates that password security is not well understood, resulting in a significant knowledge gap.

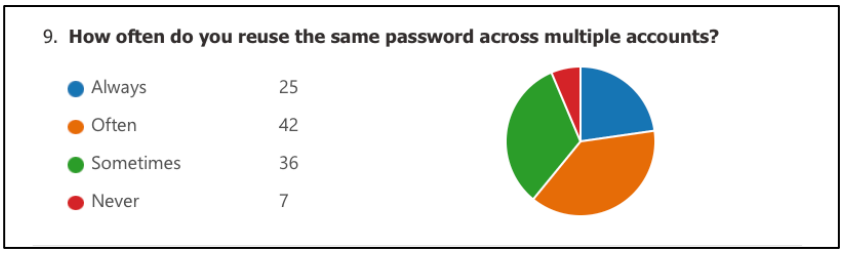

Figure 4.9: Password Reuse Practices Among Respondents

As shown in Figure 4.10, most respondents reported or ignored suspicious emails, while only a small number clicked on the link immediately. Specifically, 52 respondents would report the email, 49 respondents would ignore it, 6 respondents are not sure what to do, and only 3 respondents would click the link immediately. This suggests that most people have basic awareness, although some uncertainty still exists.

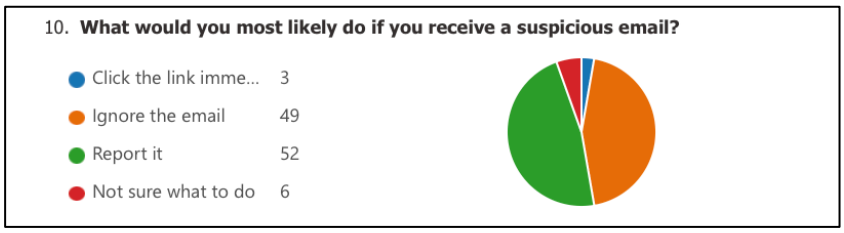

Figure 4.10: Response to Suspicious Email Scenariox

Figure 4.11 indicates that most respondents verify links before clicking them. Specifically, 45% always verify links, 27% sometimes, 16% often, and 11% never verify links. This reflects generally good awareness, although some individuals still follow unsafe practices.

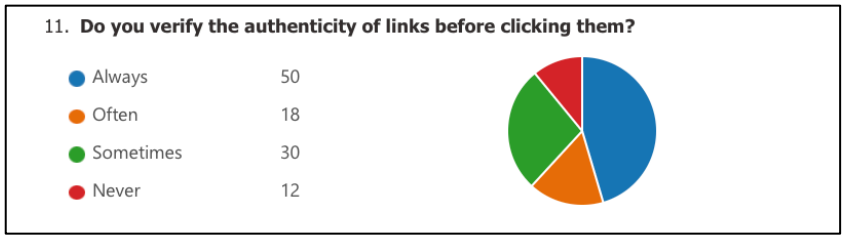

Figure 4.11: Verification of Link Authenticity Before Clicking

According to Figure 4.12, the majority of respondents rarely or never update their passwords. Specifically, 36% rarely update their passwords, 33% do so regularly, 18% occasionally, and 13% never update them. This indicates weaknesses in password management practices, which may increase security risks.

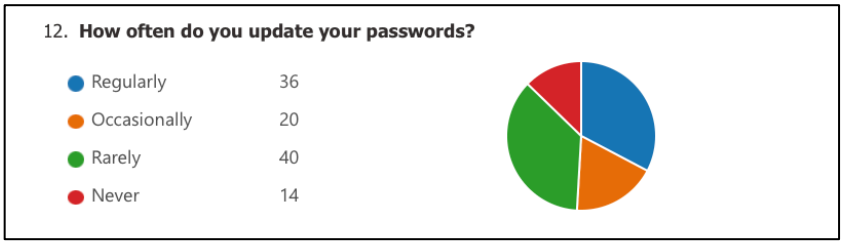

Figure 4.12: Frequency of Password Updates

Based on Figure 4.13, while many respondents follow cybersecurity best practices frequently or always, there is still inconsistency. Specifically, 46 respondents always follow best practices, 26 respondents often, 26 respondents sometimes, and 12 respondents never follow them. This shows that adherence to security practices is not consistent among users.

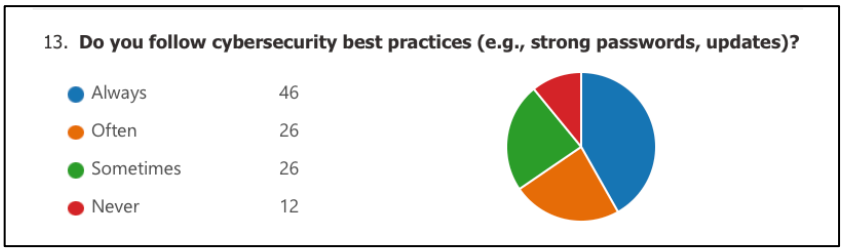

Figure 4.13: Cybersecurity Best Practices Adoption

Figure 4.14 shows that respondents strongly believe continuous cybersecurity assessment is important. Specifically, 62% consider it very important, 29% important, 9% neutral, and 0% not important. This reflects strong agreement on the need for ongoing cybersecurity evaluations.

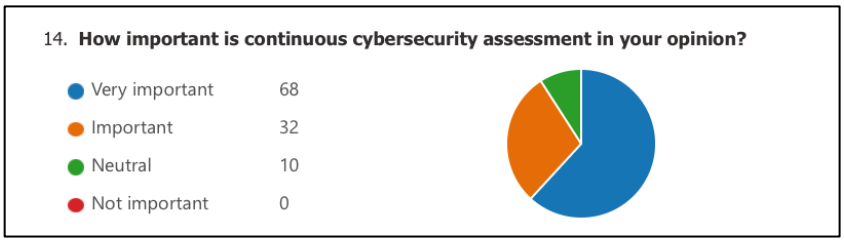

Figure 4.14: Importance of Continuous Cybersecurity Assessment

In Figure 4.15, the majority of respondents believe that personalized training would improve their security behavior. Specifically, 48% consider it very effective, 41% effective, 10% slightly effective, and 1% not effective. This shows strong support for targeted training approaches to improve cybersecurity awareness.

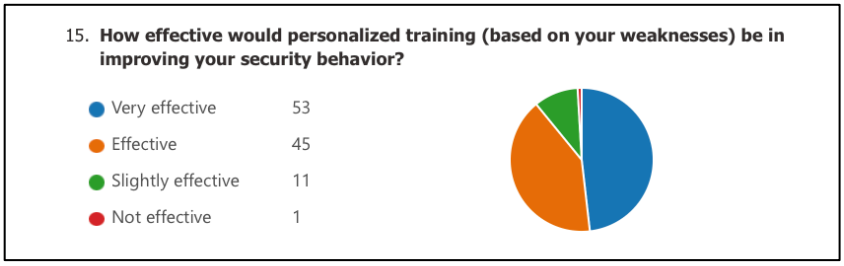

Figure 4.15: Effectiveness of Personalized Training in Improving Security Behavior

Figure 4.16 shows strong agreement that organizations should use systems to monitor and improve cybersecurity awareness. Specifically, 77 respondents strongly agree, 27 respondents agree, 4 respondents disagree, and 2 respondents strongly disagree. This reflects strong support for such systems.

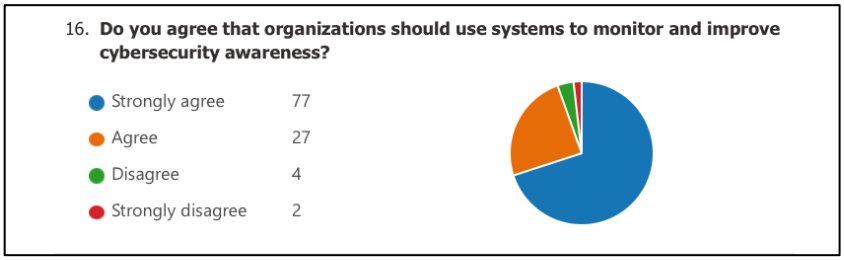

Figure 4.36: Opinion on Using Systems to Monitor and Improve Cybersecurity Awareness

As shown in Figure 4.17, most respondents believe that cybersecurity awareness should be assessed regularly or continuously. Specifically, 58% prefer continuous assessment, 30% regular assessment, 11% occasional assessment, and 1% one-time assessment. This indicates a strong preference for ongoing evaluation.

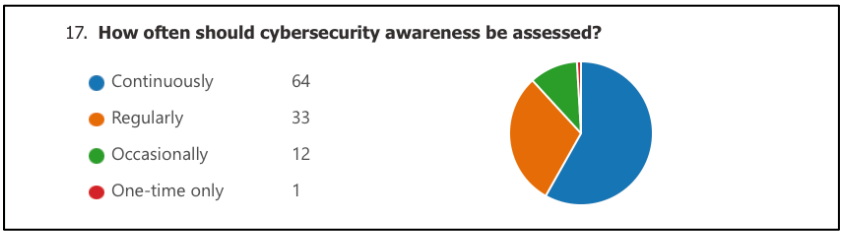

Figure 4.17: Frequency of Cybersecurity Awareness Assessment

In In Figure 4.18, most respondents support the use of systems that track cybersecurity performance and provide feedback. Specifically, 64% consider it very useful, 31% useful, 5% slightly useful, and 0% not useful. This shows strong demand for such systems.

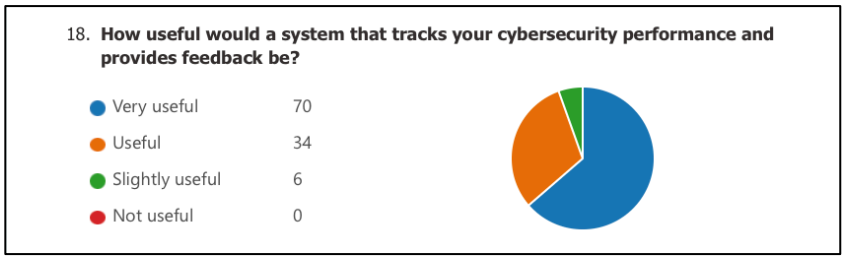

Figure 4.18: Usefulness of cybersecurity awareness tracking systems

4.2 System Requirements

Corporate CyberAware is subjected to a set of functional and non-functional requirements designed to ensure its effectiveness. The requirements describe the system's primary capabilities and the performance standards necessary to support continuous behavior-based cybersecurity awareness assessments.

4.2.1 Functional Requirements

A functional requirement describes the operations and services provided by a system and Table 4.1 shows the functional requirements for Corporate CyberAware.

ID	Requirement	Description
FR-1	Conduct Cybersecurity Assessments	Administrations will create and manage security assessments, covering topics such as phishing and password security. Employees will be able to complete these assessments, and the scores will be automatically calculated and recorded.
FR-2	Behavioral-Based Evaluation	Based on responses and interactions of employees, the system will assess employee performance. As part of behavior-oriented risk assessment, it is necessary to identify weaknesses, such as an inability to detect phishing attempts.
FR-3	Progress Tracking and Reporting	Administrators will be able to track the progress of employees over time using the system. It will provide detailed reports regarding scores, completion rates, and performance trends as part of its decision-making process.
FR-4	Role-Based Access Control	Access control should be role-based in classification to differentiate between administrators and employees. Administrators should be able to manage assessments and view reports, while employees should only be able to take assessments, complete assigned training, and view their results.

FR-5	Feedback System	Employee performance can be evaluated by administrators using the system. Based on the results, this feedback is provided to help users improve their understanding of cybersecurity issues.
FR-6	Continuous Assessment Mechanism	The system should support periodic assessments of employee awareness as part of a continuous assessment process. Creating a repository of historical performance assessment data will enable organizations to assess employee performance and identify potential risks.
FR-7	Training Module Management	Administrators should be able to create, edit, and delete training modules and assign training modules for both employees and departments.
FR-8	Employee Dashboard and Analytics	Employees should be able to view awareness summaries, assigned assessments and modules with progress, and behavioral insights through an interactive dashboard.
FR-9	Department Management	Administrators should be able to create departments and manage employees into departments for easier assignment and tracking.
FR-10	Risk Level Identification	The system should identify employee risk levels based on assessment performance and training completion.

Table 4.1: Functional Requirements

4.2.2 Non-Functional Requirements

The non-functional requirements define the system's quality attributes and constraints, and Table 4.2 shows the non-functional requirements for Corporate CyberAware.

ID	Requirement	Description
NFR-1	Security	Users should be able to authenticate securely and have their data protected. It is important to ensure that the website is protected against common vulnerabilities on the Internet.
NFR-2	Usability	Using a user-friendly interface and easy navigation, employees will be able to complete assessments more quickly, while administrators will be able to manage system functions more efficiently.
NFR-3	Performance and Reliability	System performance must be consistent without crashing, and assessment results must be stored accurately. The system requires fast-loading time for assessments and reports. Several users should be able to access the system simultaneously without experiencing significant delays.
NFR-4	Scalability	The system will be suitable for deployment in both larger and smaller organizations as it expands in terms of users and assessments.

NFR-5	Maintainability	A modular architecture will facilitate the easy updating of assessments, features, and system components without affecting overall functionality.
NFR-6	Compatibility	The system should function properly on commonly used web browsers and devices.

Table 4.2: Non-Functional Requirements

4.3 System Models

This section provides visual illustrations of CyberAware architecture to describe its functionalities, user interactions, and data operations. It includes the system architecture data flow diagram (DFD), and entity-relationship diagram (ERD) to show how the system is structured and how its components work together.

4.3.1 System Architecture

The system is structured into a three-tier architecture as shown in Figure 4.19, including a presentation layer, an application layer, and a database layer. The presentation layer is crafted using HTML, Tailwind CSS, and JavaScript to provide both administrators and employees with a clear and easy user experience.

The backend tier is developed using Python Flask and created APIs that handle user management, assessment creation, AI-based assessment and training module generation, performance evaluation, and training management. The AI is developed using chatbase and intended to help in generating assessments and training modules.

The database layer uses mySQL to store users, departments, assessments, results, training materials, and profile change. The communication between tiers is carried out using HTTP requests, where the frontend forwards user (employee) actions to the backend to process the data and interacts with the database before sending results to the user (admin).

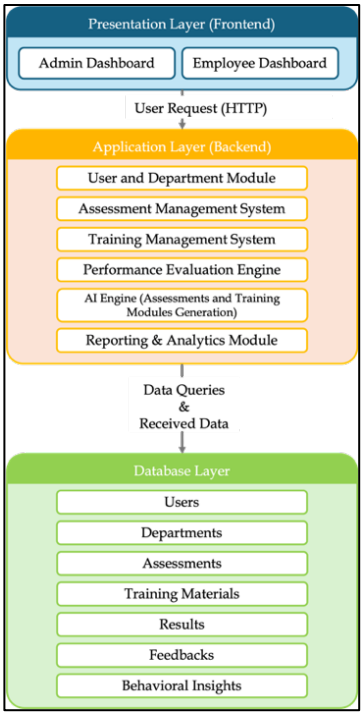

Figure 4.19: System Architecture Diagram

4.3.2 Data Flow Diagram (DFD)

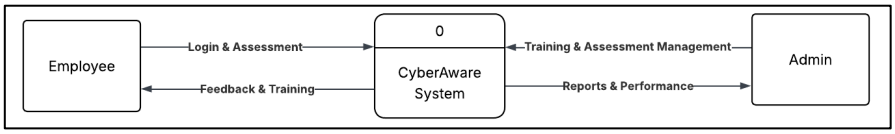

Figure 4.20: Level 0 CyberAware Data Flow Diagram

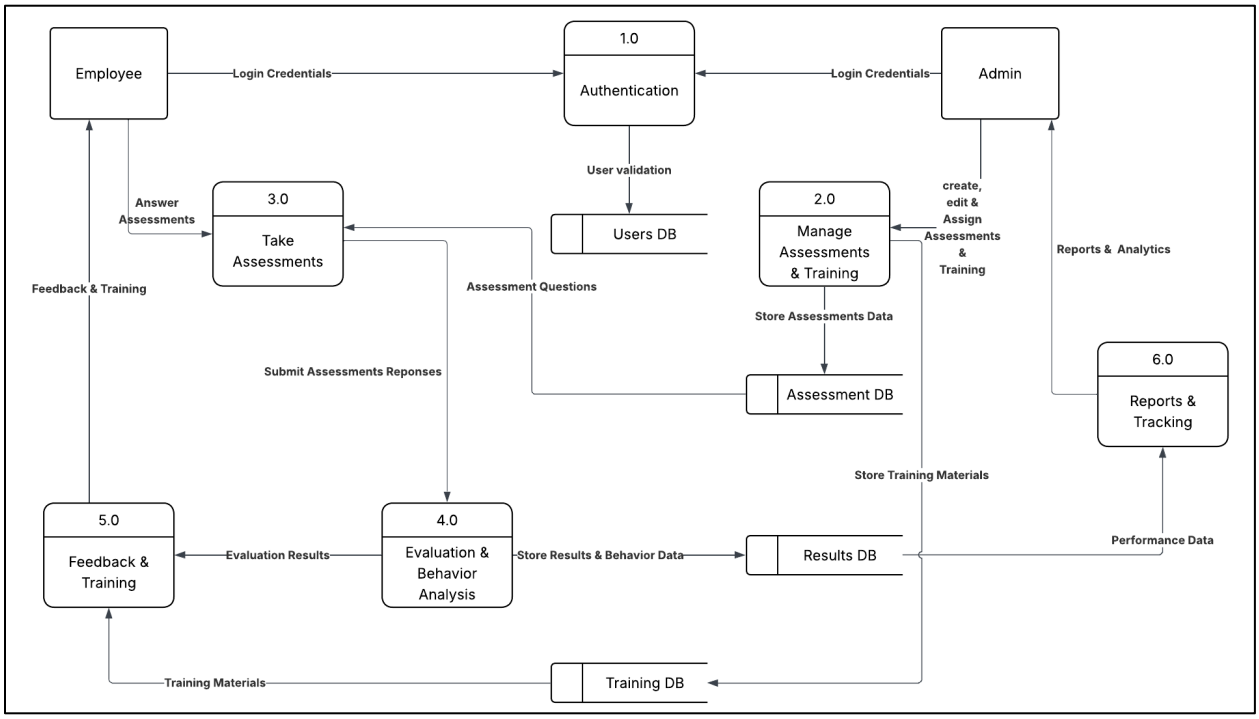

Figure 4.21: Level 1 Cyberaware Data Flow Diagram

Figure 4.20 and Figure 4.21 presents the Data Flow Diagram (DFD) for our system "Corporate CyberAware." It illustrates the flow of data between entities, processes, and data stores for a clearer understanding of system operation.

The Level 0 context diagram in Figure 4.20 provides an overview of the system's interaction with external entities, including "Admin" and "Employee". The admin creates, edits, and assigns assessments and training materials, receiving analytics, and generating reports. The Employee logs in, completes assessments, views training modules and receives feedback.

In level 1 shown in Figure 4.21, the detailed DFD shows the internal structure of the system. The first process (Authentication 1.0) is to validate the user's credentials, and that happens by accessing the user's database. Once the user is authenticated, the employee can take assessments, which is the third process; the assessment questions are retrieved from the assessment database.

The process (Manage Assessments & Training 2.0) lets the admin create, edit, and store assessment data and training materials and store them in their respective databases. The submitted assessment responses are processed and analyzed in the (Evaluation and Behavior Analysis 4.0) process, the scores are also calculated, and the employee's behavior is evaluated. Then, the results are stored in the results database.

The (Feedback & Training process 5.0) process retrieves suitable training materials from the training database and admin generates feedback based on the evaluation results. In the end, the (Reports & Tracking 6.0) process creates reports and analytics for the admin using performance data from the results database.

Overall, the DFD diagram indicates that the system facilitates ongoing assessments, behavior-based evaluation, and customized cybersecurity awareness through a systematic data flow.

4.3.3 Entity Relationship Diagram (ERD)

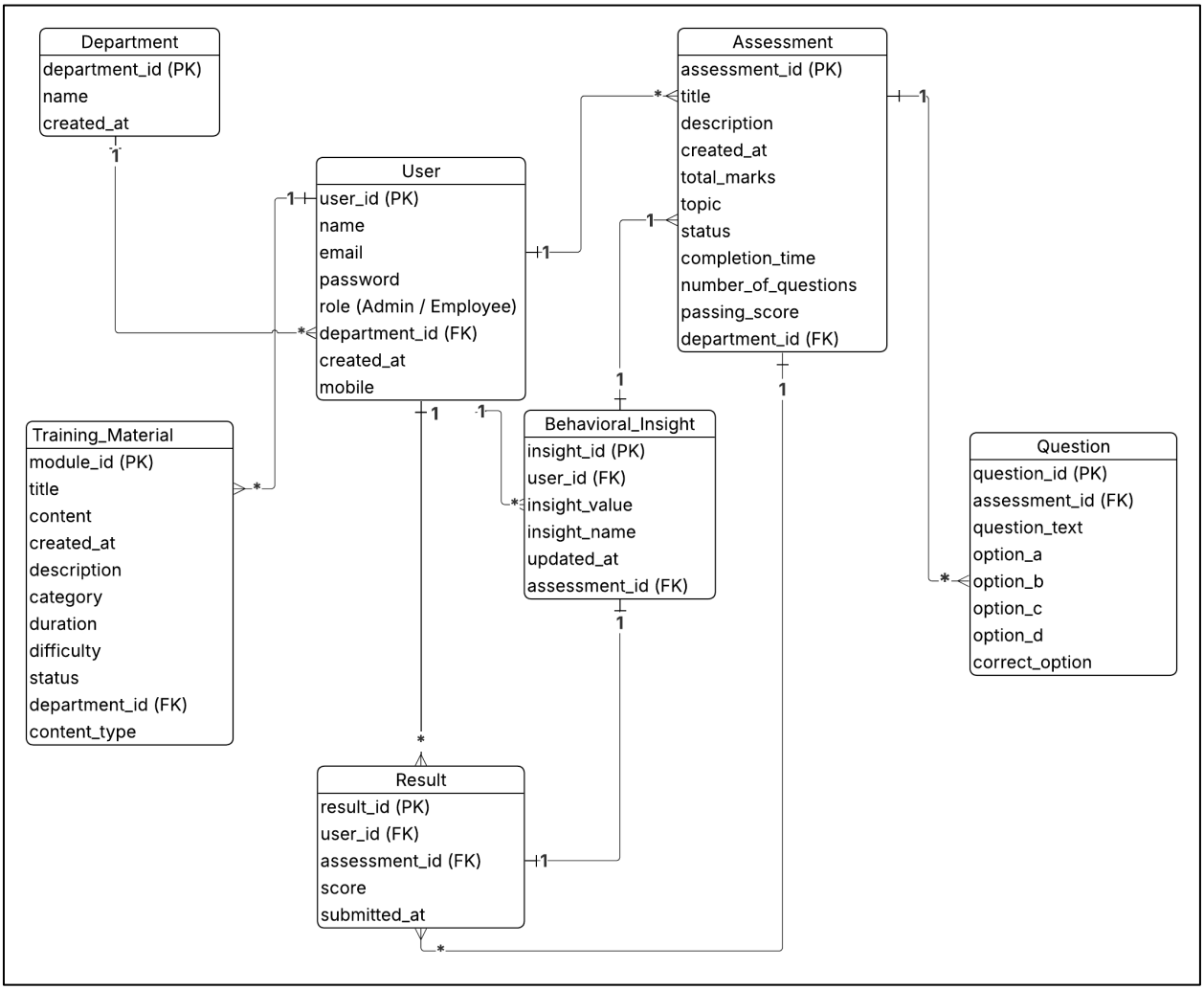

Figure 4.21: Cyberaware Entity relationship Diagram

The Cyberaware system's Entity Relationship Diagram (ERD) in figure 4.21 outlines the database's structure and relationships among entities. The system has seven primary components: User, Department, Assessment, Question, Result, Training_Material, and Behavioral_Insight. The User entity is for both the admin and employee, and it is differentiated by the role attribute. User "Employee" is linked to a specific Department, establishing a one-to-many relationship where a single department can have multiple users "Employees".

The admin creates and assigns assessments and stores them in the Assessment entity. The created_at and department_id attributes link each assessment to a user. The Question entity contains the assessment-related questions along with multiple-choice answers and the correct solution. Assessment and Question entities have a one-to-many relationship in which a single assessment has several questions.

The results of user assessments are stored in the Result entity. Score and submitted_at attributes are among its features that aid in behavior-based analysis along with the Behavioral_Insight entity that relates to both Assessments and Results entities to also help with ongoing analysis. There are one-to-many relations between User-Result entities, and Assessment-Result entities, since each result is linked to a single user and assessment. In addition, there are one-to-one relationships between Result-Behavioral_Insight entities, and Behavioral_Insight-Assessment because each result is connected with one behavioral insight and each assessment provide one behavioral insight.

Admin creates training content and stores it in the Training_Material entity. The entity stores the training content categorized by its difficulty, content type, and duration. The linkage between Training_Material and departments by category covers the requirement of "customized educational content" depending on the awareness deficiencies. The User and Training_Material have a one-to-many relationship, which means that one admin can create and edit multiple training materials.

The ERD exhibits a logical database design that promotes the system's fundamental functions, such as assessment management, performance tracking, and behavior-based cybersecurity awareness improvement.

Chapter 5: System Design

5.0 Introduction

This chapter explains how the Corporate CyberAware system is designed. It shows how the system works, how its parts are connected, and how users interact with it. It also includes the database design, user interface screens, and main system processes.
This system is designed to be simple and easy to use, providing employees with the ability to complete assessments, access training, and view their feedback without difficulty.

5.1 Database Schema Design

The database for Corporate CyberAware is designed to manage employees, training modules, and assessments in an organized way. It follows a relational structure where tables are connected using primary and foreign keys. This helps keep the data consistent and easy to manage across the system.

5.1.1 User and Organizational Management

Departments table

Field Name	Description
department_id	Primary Key
name	Department name
created_at	Record creation timestamp

Table 5.1: Departments table

Employees table

Field Name	Description
employee_id	Primary Key
name	Employee full name
email	Unique email address
password_hash	Employee password
department_id	Foreign Key (links to Departments)
role	User role (admin/employee)
created_at	Record creation timestamp
mobile	Employee Mobile Number

Table 5.2: Employees table

admin_profile Table

Field Name	Description
Admin_id	Primary Key
name	Admin full name
email	Admin email
mobile	Admin mobile number
password_hash	Admin account password

Table 5.3: admin_profile table

The Departments, Employees, and Admin Profile tables manage the organizational structure and admin accounts in the system. Employee are linked to a department using the department_id, to organize assessments and training modules. The Admin Profile table stores administrator information used to access the system, manage and monitor the platform.

5.2.2 Training Module Management

module table

Field Name	Description
module_id	Primary Key
title	Module title
description	Module description
content	Training content
category	Module Category
duration	The estimated time to complete the training module
difficulty	Level of difficulty(Beginner, Intermediate, Advanced)
status	Module status (Published, Draft, Advanced)
department	Assigned departments to that module
content_type	The type of the content in the module (Video, Slides, Document/PDF, Scenario)
created_at	Timestamp of creation

Table 5.4: module table

assigned_modules Table

Field Name	Description
assignment_id	Primary Key
employee_id	Foreign key (Employees table)
module_id	Foreign key (Module table)
department_id	Foreign key (Department table)
status	Progress status (Not Viewed/completed)
assigned_at	Assignment timestamp

Table 5.5: assigned_modules Table

The Module table contains the training content, while assigned_modules connects employees to the modules they are assigned. This allows the system to track each employee taking a module and how they have progressed. It helps in monitoring training completion in a simple and clear way.

5.2.3 Assessment Management

A- Assessment and Questions (Core content layer):

Assessments Table

Field Name	Description
assessment_id	Primary Key
title	Assessment title
total_marks	Maximum marks
created_at	Timestamp
topic	Assessment topic
status	Assessment creation status
completion_time	The estimated time to answer the assessment
number_of_questions	Number of questions in the assessment
passing_score	The minimum score to pass
description	Assessment description
department	Assigned departments to that assessment

Table 5.6: Assessments Table

Questions Table

Field Name	Description
question_id	Primary Key
assessment_id	Foreign key (Assessments table)
question_text	Question content
option_a	Option A
option_b	Option B
option_c	Option C
option_d	Option D
correct_option	Correct answer

Table 5.7: Questions Table

Assessments are used to test employee understanding of cybersecurity. Each assessment contains multiple questions, and each question belongs to a specific assessment through the assessment_id. This structure allows proper evaluation of employee knowledge.

B. Employee_Assessments (tracking layer):

assigned_assssments Table

Field Name	Description
assignment_id	Primary Key
employee_id	Foreign key (Employees table)
assessment_id	Foreign key (Assessments table)
department_id	Foreign key (Departmentstable)
assigned_at	Assignment timestamp

Table 5.8: assigned_assssments Table

The assigned_assssments table if for the admin to assign assessments to multiple departments and employees. This helps in managerial aspects where admin can manage assessments.

5.2.4 Employee Performance and Results

a. Answers, Assessment Results and Assessment Feedback:

answers Table

Field Name	Description
answer_id	Primary Key
employee_id	Foreign key (Employees table)
question_id	Foreign key (Questions table)
selected_option	Selected answer
is_correct	Correctness indicator

Table 5.9: answers Table

assessment_results Table

Field Name	Description
result_id	Primary Key
employee_id	Foreign key (Employees table)
assessment_id	Foreign key (Assessmentstable)
score	Employee score
Submitted_at	Correctness indicator

Table 5.10: assessment_results Table

assessment_feedback Table

Field Name	Description
feedback_id	Primary Key
employee_id	Foreign key (Employees table)
assessment_id	Foreign key (Assessmentstable)
feedbback	Feedback from the admin
Submitted_at	Correctness indicator

Table 5.11: assessment_feedback Table

The Answers table records each employee's response to a question. This allows deeper analysis of performance beyond the final score. Then the scores are saved in assessment_results Table. Based on the score the admin provides the employee feedback that is also stored in assessment_feedback Table.

b. Behavioral Insights:

behavioral_insights Table

Field Name	Description
insight_id	Primary Key
employee_id	Foreign key (Employees table)
insight_name	The name of the insight(changeable)
insight_value	The calculated value of the insight
updated_at	Last time updated

Table 5.12: behavioral_insights Table

The Table behavioral_insights shows the cybersecurity behavioral insights for each employee and helps admin to review awareness patterns and identify high level risk employees and assign training modules based on the insight.

Relationships Overview

The database is built using connected tables to keep data consistent. Employees belong to departments, modules are created for training, and assessments. Questions are attached to assessments, while employee performance is tracked through training progress, and assessment results. All these connections work together to give a complete view of employee cybersecurity awareness.

5.2 User Interface Design

5.2.1 Login Interface Design

The login interface shown in Figure 5.1, supports both the admin and employee to login into Corporate CyberAware system using their account credentials. “Farah” can login to the system as admin, and “Yaqoob” login as an employee.

Features:

- Email input field
- Password input field
- A link to Sign up page
- Login button (Get Started)

Yaqoob enters his corporate credentials (email and password) to access the system. After submitting his credentials, the system verifies his identity and grant him access to his dashboard. The simple and clear interface helps Yaqoob to complete login process quickly.

In the admin side, Farah can enter her corporate credentials the email and its corresponding password to let the system verify her identity and grant her access to the dashboard. If the admin does not have an account, he should click the sign-up link to create an account and access Corporate CyberAware system.

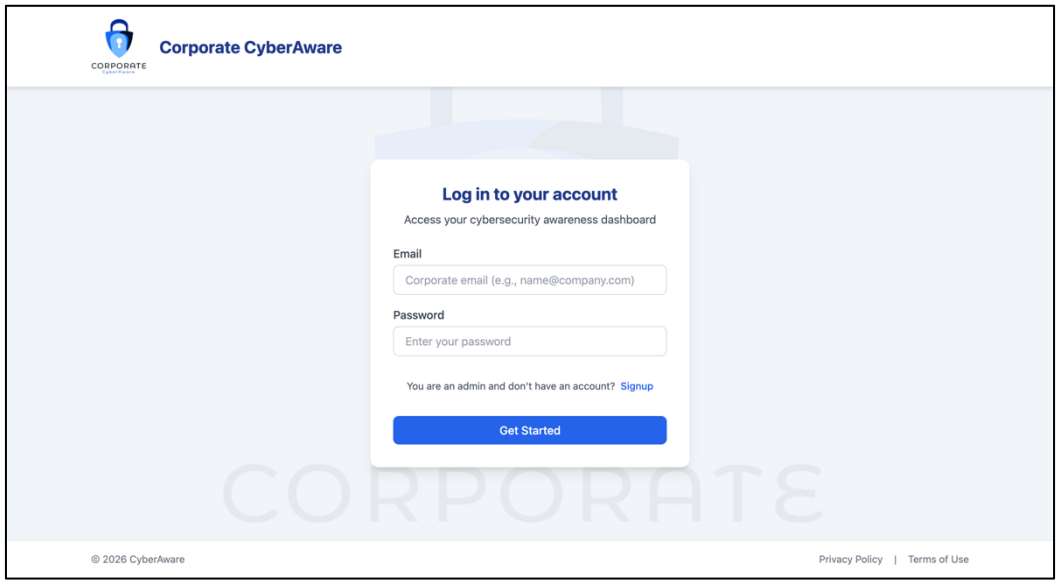

Figure 5.4: Login Page

5.2.2 Employee Interface Design

5.2.2.1 Employee Dashboard

In Figure 5.2, the page represents the main dashboard where the employee "Yaqoob" can view his cybersecurity awareness status and access system features.

Features:

- Sidebar navigation (Dashboard, Assessments, Training, Analytics, Profile, Logout button)
- Risk alert notification
- Awareness Summary (Assigned Assessments and Training Modules, Awareness Level, Overall Progress)
- Pending actions (Assigned Assessments and Training Modules)
- Behavioral insights (Awareness Status, Behavioral Trend, Average Score, Completion Progress, Completed Assessments and Training Modules)

After successfully logging in, Yaqoob is directed to the dashboard where he is welcomed and presented with an overview of his cybersecurity awareness status. He can view the navigation bar on the side, which allows him to access different sections of the system. In addition, he notices a risk alert notification with recommended actions. Yaqoob can review his awareness level, track his progress, and view his behavioral insights. He can also access pending actions such as completing assessments, and training.

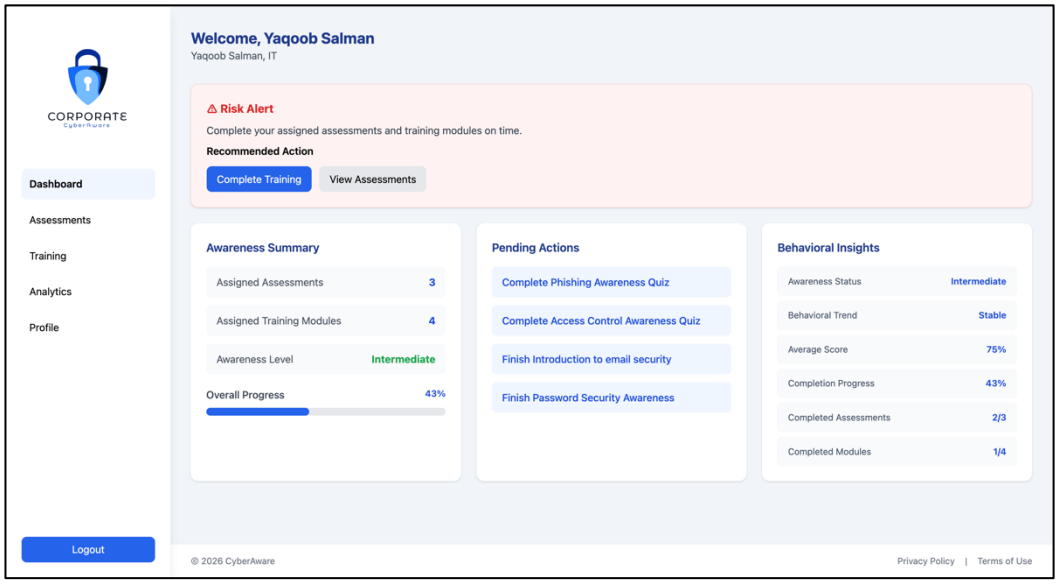

Figure 5.2: Employee Dashboard

5.2.1.3 Assessments Page

According to Figure 5.3, the page allows the employee "Yaqoob" to view and manage his assigned cybersecurity assessments.

Features:

- Search and filter assessments
- Employee Assessment Progress Bar
- List of assessments with title, topic, number of questions, grade, and status
- Start or restart assessment buttons
- Recent results and feedback section

From the dashboard, Yaqoob navigates to the assessments page, where he can search for specific assessments or filter them based on topic or status. He can select an assessment to start or restart depending on its progress. Also, he can review his recent results and access feedback to better understand his performance.

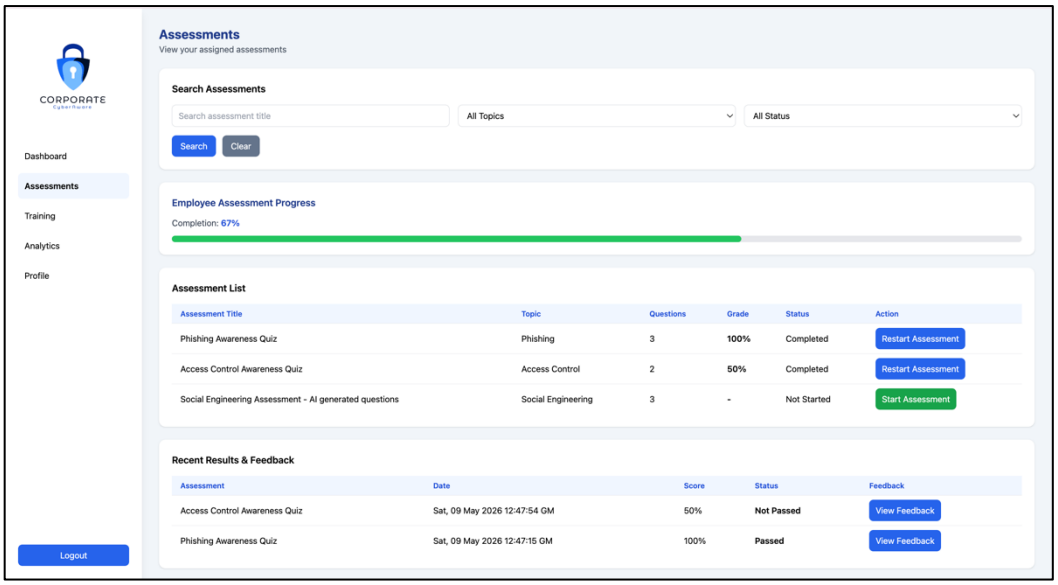

Figure 5.3: Assessments Page

5.2.1.4 Training Page

Figure 5.4 shows the training page. This page allows the employee “Yaqoob” to access and complete cybersecurity training modules.

Features:

- Search and filter Training modules
- Training progress bar
- List of training modules
- Status indicator (completed or not viewed)
- Action buttons (start, review module)

After reviewing his assessments, Yaqoob navigates to the training page to improve his weak areas. He can track his overall training progress and clearly see the status of each training module. Yaqoob starts new modules, or reviews completed ones, helping him gradually improve his cybersecurity awareness and behavior.

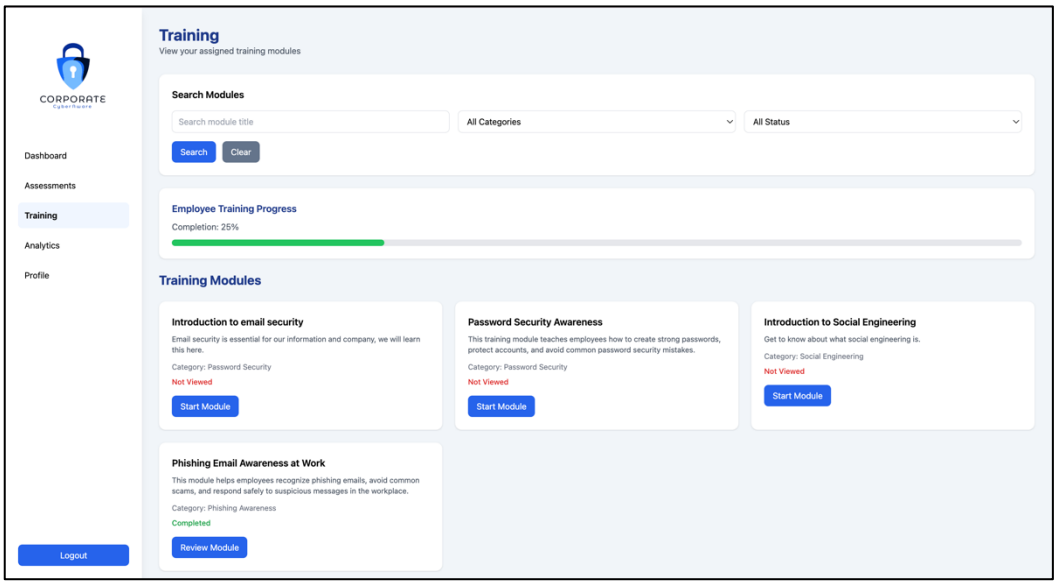

Figure 5.4: Training Page

5.2.1.5 Analytics Page

According to Figure 5.5, this page allows the employee “Yaqoob” to view detailed analytics about his cybersecurity behavior.

Features:

- Awareness score, risk level, training completion, completed assessments
- Assessment progress trend chart
- Risk behavior distribution chart
- System recommendations

After completing the assessments and training, Yaqoob visited the analytics page to understand his performance in more detail. He clearly can see his scores, risk level, and progress overtime

through visual charts. The system also highlights risky behaviors and provides recommendations, helping Yaqoob focus on improving specific weaknesses.

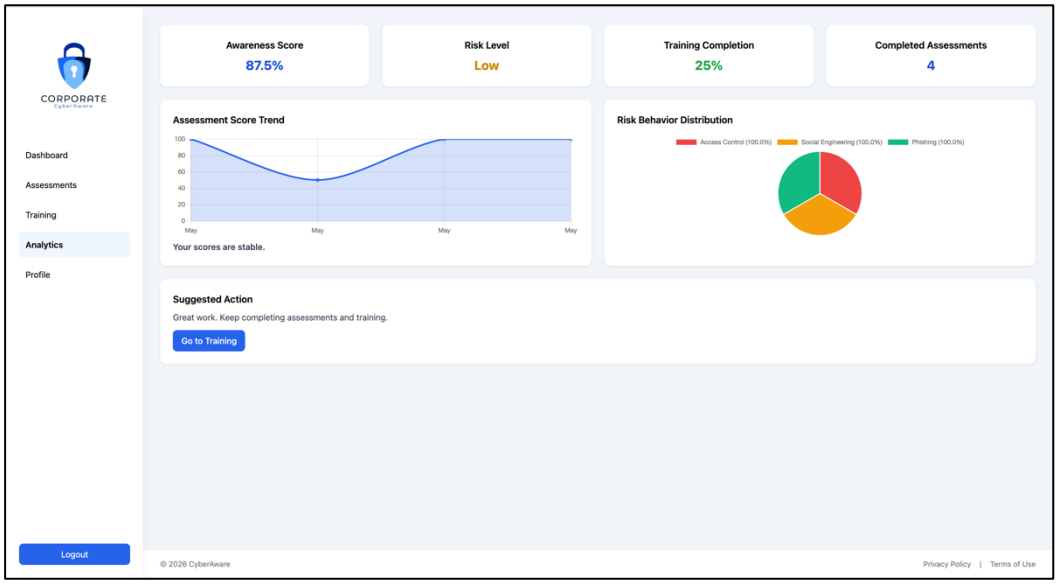

Figure 5.5: Analytics Page

5.2.1.6 User Profile Page

In Figure 5.6, it shows the user profile page, where it allows the employee "Yaqoob" to view and manage his personal account information.

Features:

- Profile information (name, email, role, department, mobile number)
- Update mobile number button

At this stage, Yaqoob navigates to his profile to manage his personal information. He can update his mobile number.

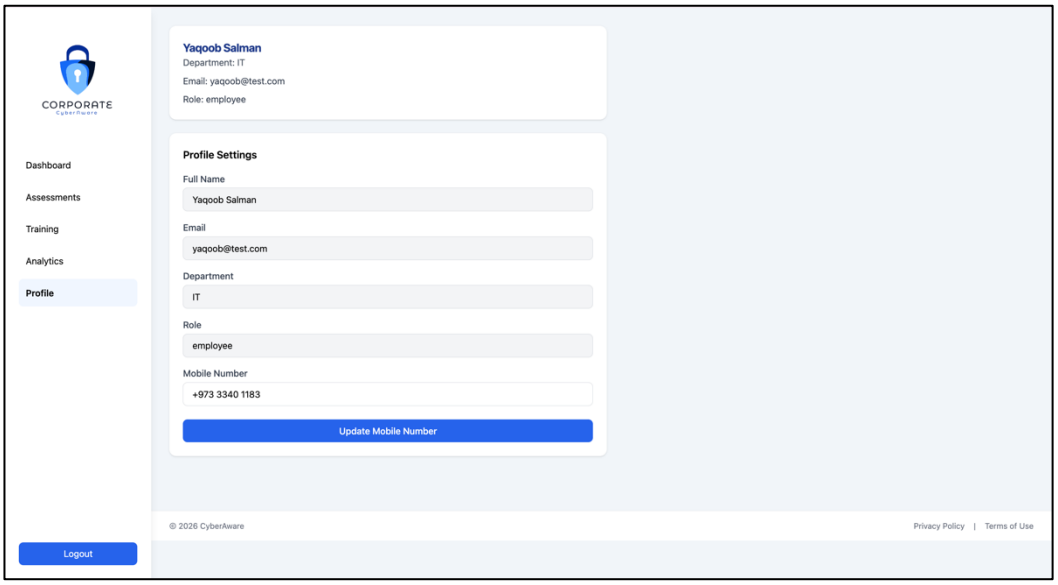

Figure 5.6: User Profile Page

5.2.3 Admin Interface Design

On the admin side, the administrator interacts with the system through multiple interfaces, allowing the admin full control to manage employees, departments, assessments, and training modules.

5.3.2.1 Sign up

Based on figure 5.7, the signup page lets the admin (Farah) create an account in the corporate CyberAware system.

Features:

- The organization name input field
- Admin full name input field
- Email input field (in a corporate email format)
- Password input field
- Confirm password input field
- Create account button
- Link to login if already have an account

First, Farah opens the sign-up page and registers for a new account for her organization. Farah enters the organization's name, her full name, and the corporate email address. She sets a password and makes sure that it is secure and then confirms it in the next input field. After that, Farah clicks the create button and successfully creates the account and accesses the system. If Farah already has an account, she can go to the login link to access the system straight away.

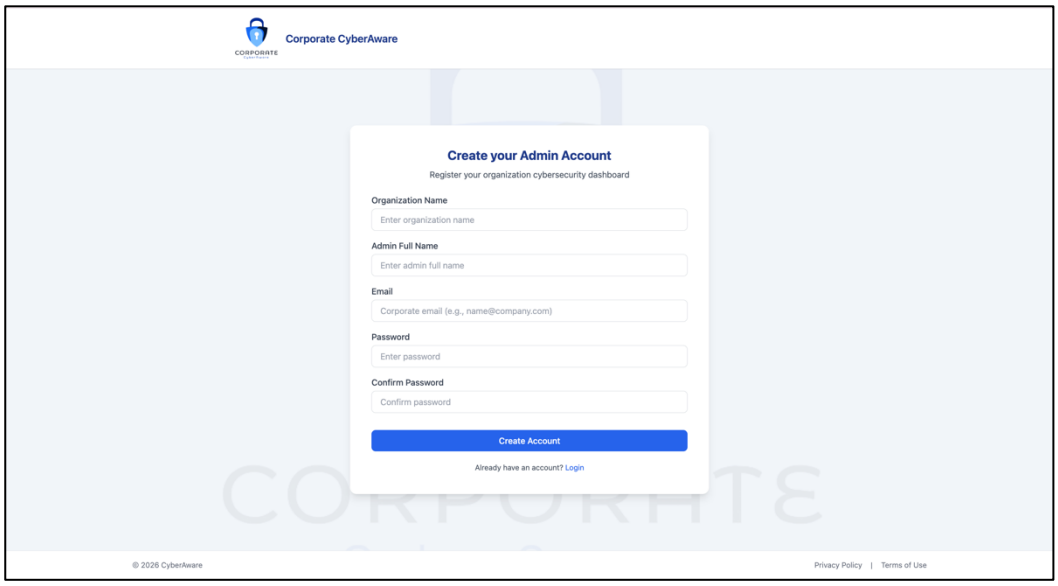

Figure 5.7: Signup page

5.2.2.2 Admin Dashboard

Figure 5.8 and Figure 5.9 show the dashboard where the admin can manage and monitor the organization's cybersecurity awareness.

Features:

- Navigation sidebar (Dashboard, Track Employees, Manage Assessments, Training Modules, Manage Employees, Profile, Logout button)
- Cards of summary overview (Total Employees, Total Departments, Total Assessment, Training Modules)
- Security risk alert with a recommended action (view risk report)
- Organizational Behavioral Overview
- Pending admin actions (Add Assessment and Training, Manage Employees)
- System Overview Card
- Quick Links
- Behavior insights
- Quick Link Departments
- Recent Assessments

After logging into the system, Farah is sent to the dashboard page. On the page, there is an overview display of the organization's overall cybersecurity awareness. The main statistics are shown on the page, and Farah can quickly view the number of employees' and departments, and total assessments and training modules. The system has a security risk alert that provides recommended actions to the highest risk level employees. Also, Farah can compare the performance of departments and monitor behavior insights helping her manage the overall progress of the organization and taking security awareness initiatives. Quick links are distributed among the dashboard.

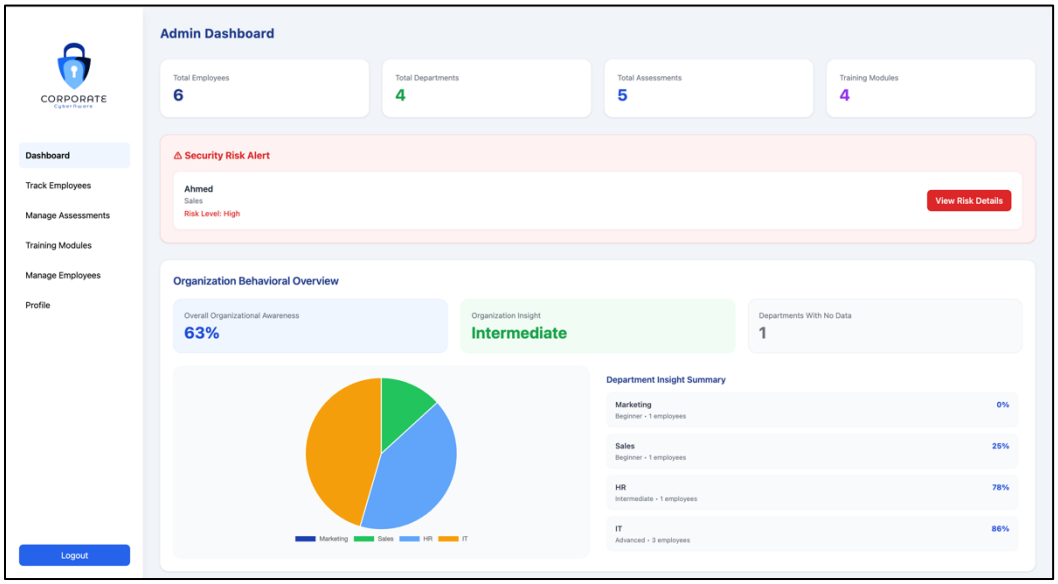

Figure 5.8: 6 Admin Dashboard

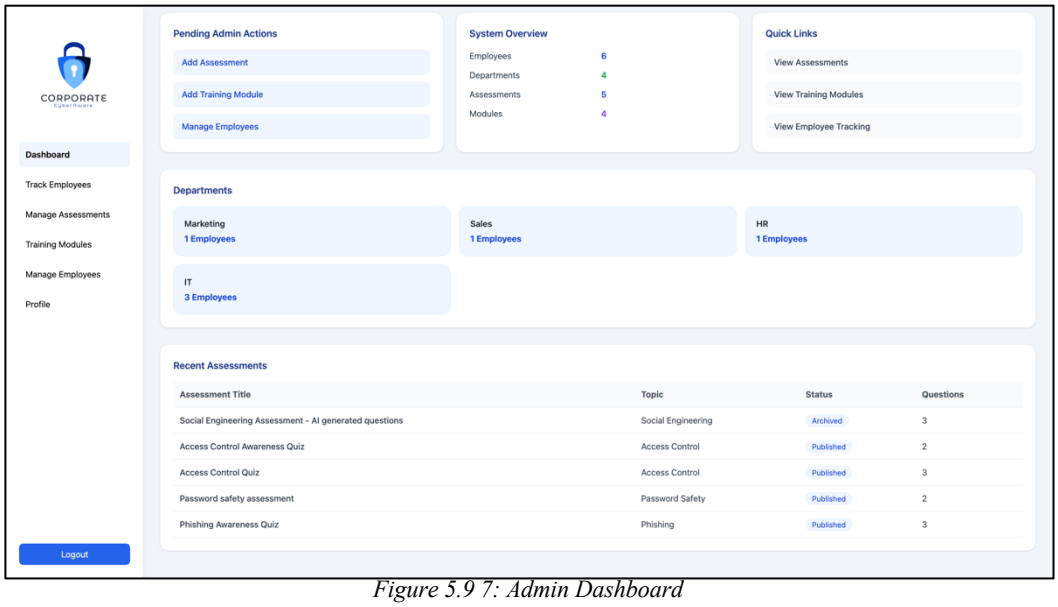

Figure 5.9 7: Admin Dashboard

5.2.2.3 Track Employees

Figure 5.10 shows how the admin track employees. It shows the organization employees.
Features:

- A search bar to find the employee by name
- Display table of employee's name, department, and action
- View button to display employee details
- Add assessment and Add module buttons

Farah can view the list of all employees in the organization and their departments; she can also search for any employee by name. Clicking on the “view” button, Farah is directed to the employee’s details page as shown in figure 5.11. The employee details page will let Farah view the employee information, employee behavioral insights, their assigned assessments and training modules alongside with their status. Farah can assign assessments and modules to the employee directly and she can also view the performed assessments.

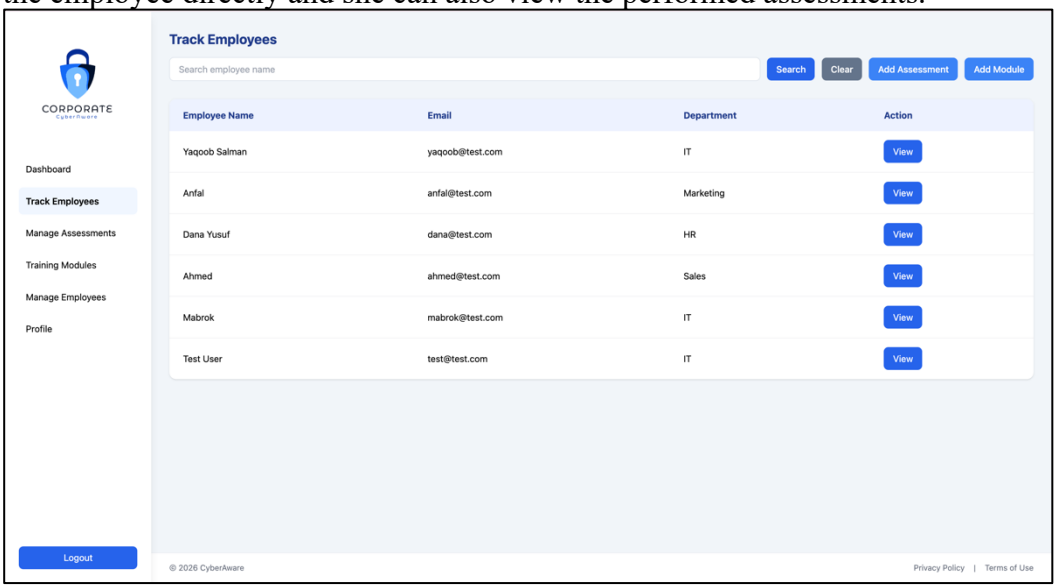

Figure 5.10: Track Employees Page

Features in Figure 5.11:

- Employee information card (name, email, department)
- Employee insights
- Assigned assessments, view button, and add assessment button
- Assigned modules with add module button

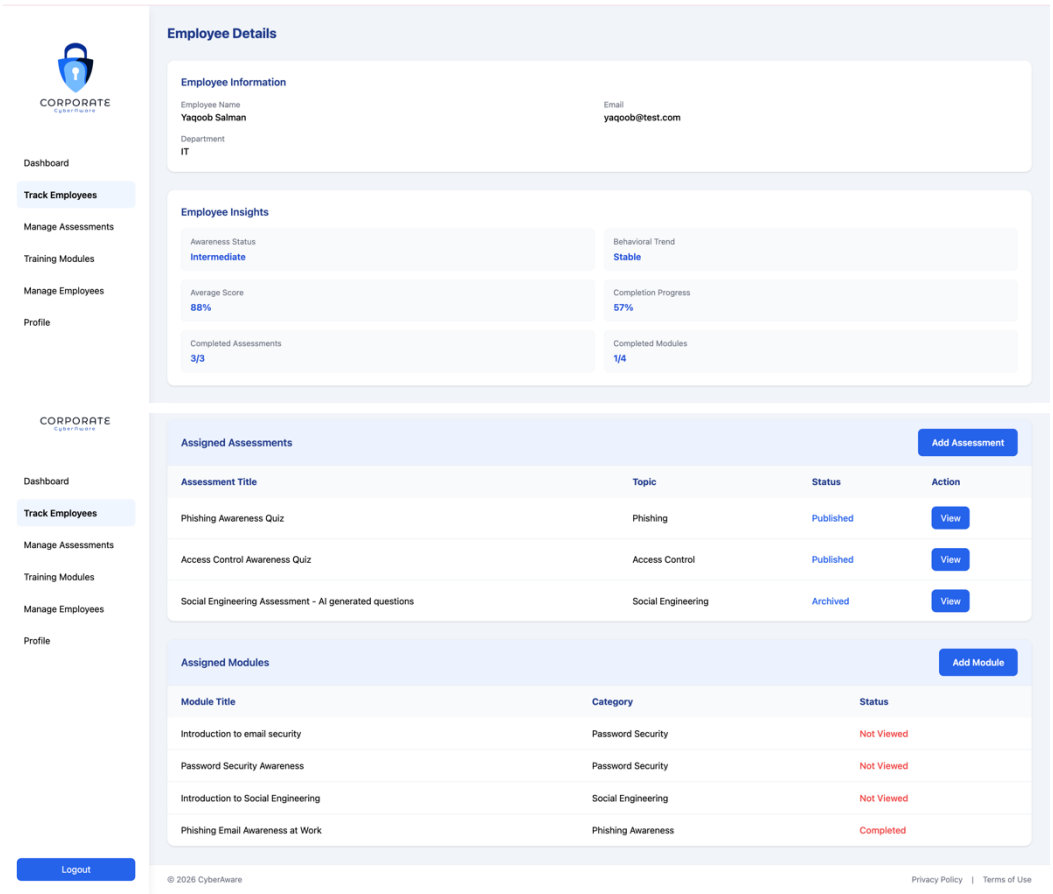

Figure 5.11: Employees Details Page

Features in Figure 5.12:

- Assessment name and employee score
- Submitted answers card
- Generate report button
- Add feedback field

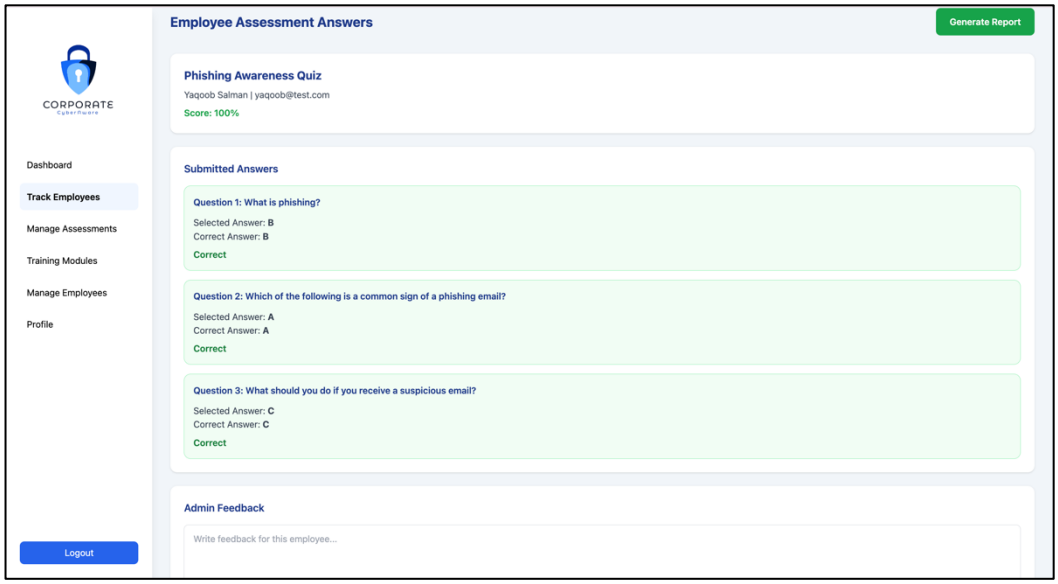

Figure 5.12: Employee Assessment Answers

In Figure 5.12, Farah can view employee's assessment answers and post feedback. She also can generate a report for the assessment for future purposes.

5.2.2.4 Manage Assessments

In Figure 5.13, the page allows the admin to create, edit, and delete assessment. In figure 5.14, the add assessment page lets the admin create a new assessment.
Features for Figure 5.13:

- Cards displaying total number of assessments, published assessments, and draft assessments
- A card that displays assessment information including assessment title, assigned department, topic, duration, status, number of questions, created at, and actions
- Add new assessment button
- Edit and delete action buttons

Features for Figure 5.14:

- New assessment creation form with answer and question options
- AI chatbot

Farah can view all assessments created after clicking the Manage Assessment button; she can review the assessment details with duration, number of questions, and the status. Farah can edit existing assessments or delete them when they are no longer needed. When clicking the Add New Assessments button, Farah is redirected to a form where she can enter assessment details like the title, topic, status, estimated completion time, number of questions, passing score, and assessment description. Farah can use the AI to create multiple-choice questions and select the correct answers.

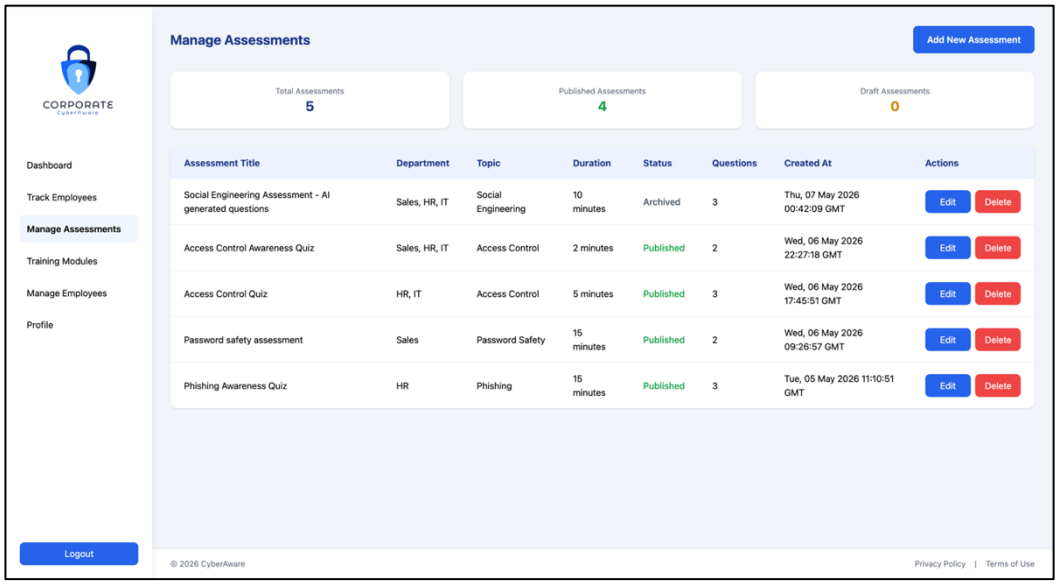

Figure 5.13: Manage Assessments page

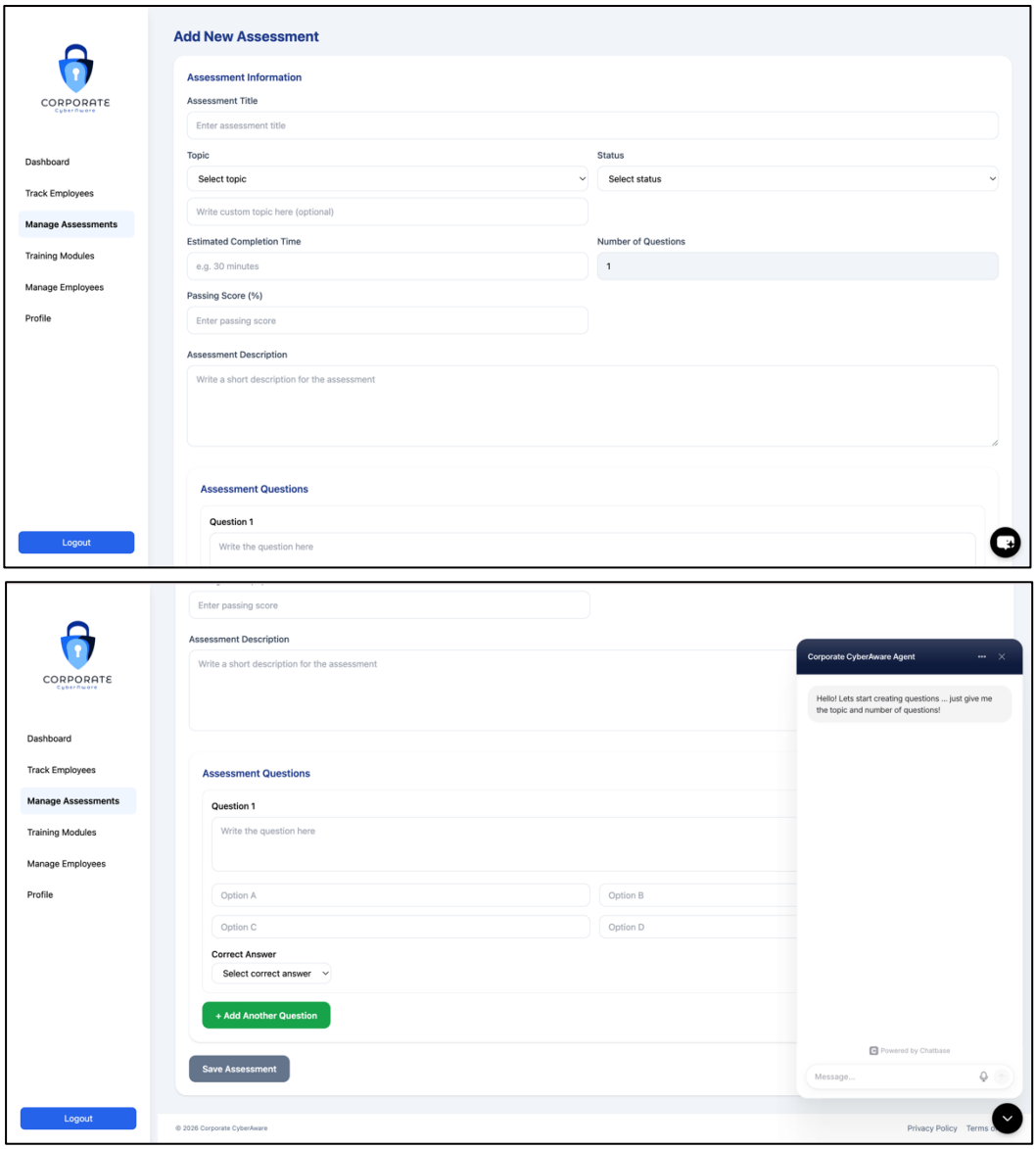

Figure 5.14: Add New Assessment with AI-Chatbot

5.2.2.5 Training Modules

Figure 5.15 shows the training module page that allows the admin to create, edit, and delete cybersecurity training modules.

Features:

- Cards displaying total number of training modules, published modules, and draft modules
- Display of training modules (title, category, duration, department, status, and actions)
- Action field with two options (Edit and delete)
- Create module button

Farah can navigate to the training modules page and view all training modules. In each module, there are details displayed like category, duration, and assigned department. As well as analytics like total modules, number of published modules, and number of draft modules. In figure 5.16 is the page that opens when Farah clicks on the "create module" button. Farah can add a new module and enter the needed details with the help of AI-Chatbot that is specifically made for creating training modules, like the title, topic, estimated duration, difficulty level, module status (published, draft, archived), and module description. The content type can also be selected (either slides, scenario training, documents/PDFs, or videos).

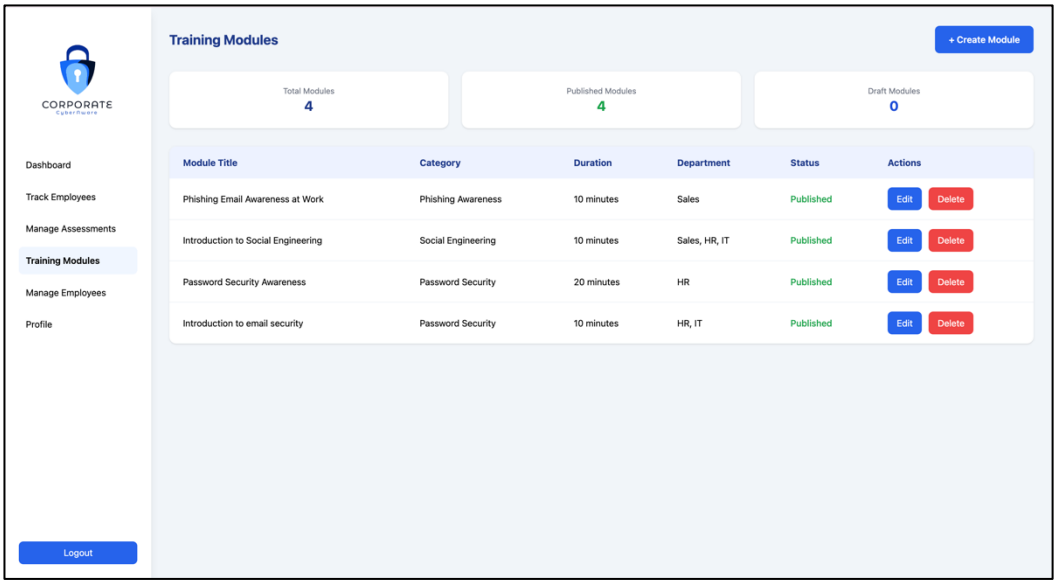

Figure 5.15: Training Modules Page

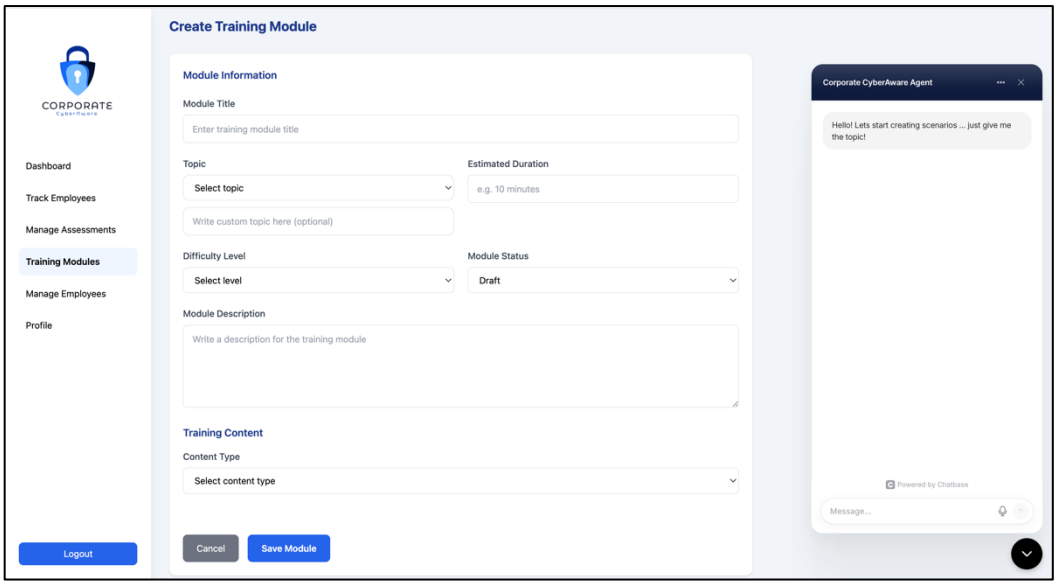

Figure 5.16: Create Training Module Page

5.2.2.6 Manage Employees

On the manage employees page, Figure 5.17 shows the departments and lets the admin manage the departments and their employees in the organization. Figure 5.18 shows the details of the department and its employees.

Features in Figure 5.17:

- Display of departments and their ID
- Add department and Remove department buttons

Features in Figure 5.18:

- Department employees list with name, role, email, actions, mobile, and insight
- View and Remove Action buttons
- Department insights (department awareness, average score, and number of employees)

Farah navigates to the manage employees page and views all the organization's departments. After selecting a department, she can view the employees with their name, role, corporate email, mobile number, actions, and behavioral insights. When clicking view button, she can view the employee progress. Farah can remove or add employees.

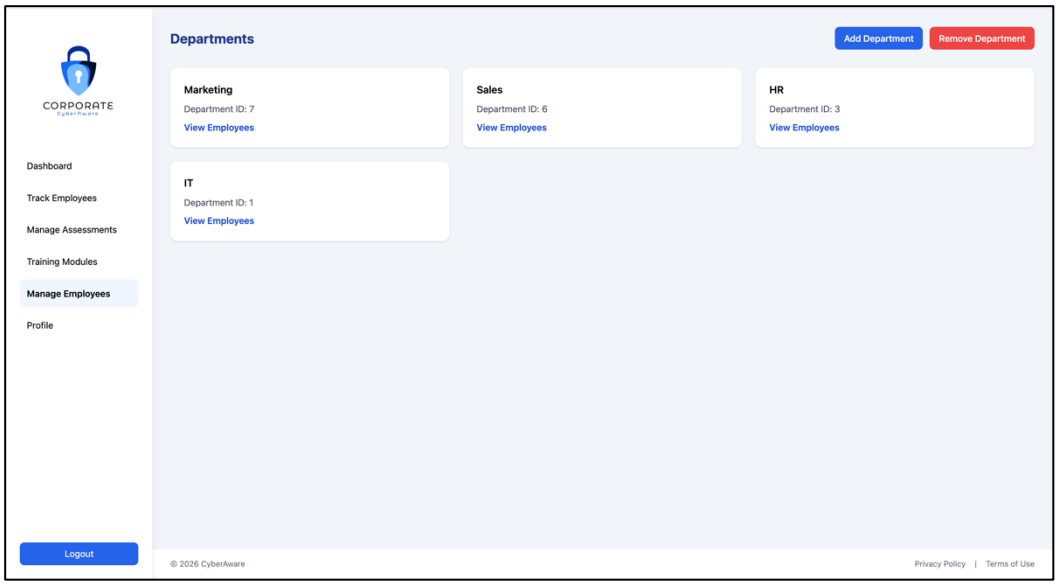

Figure 5.17: Manage Employees Departments Page

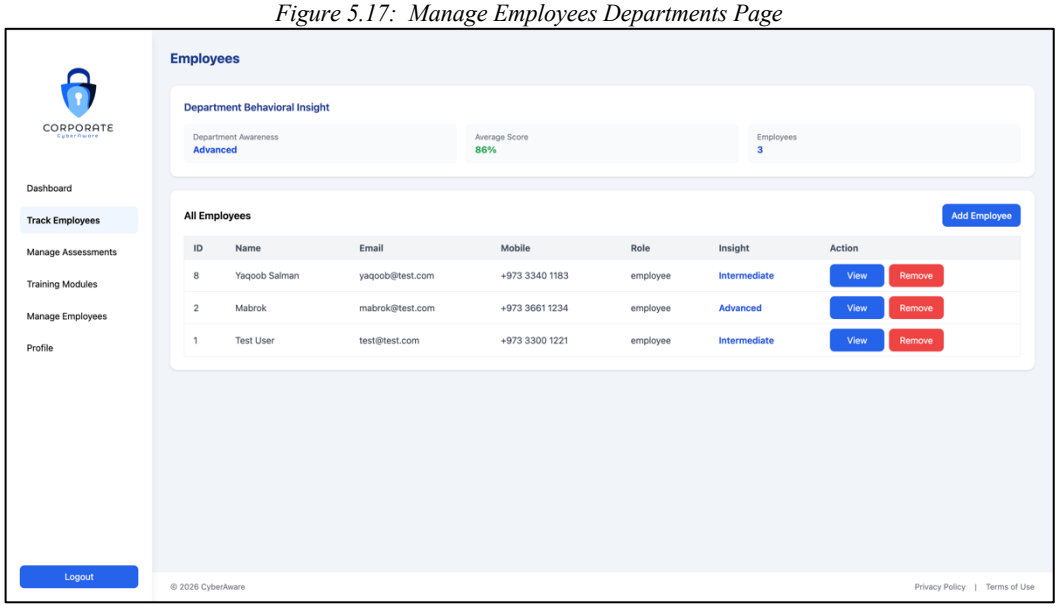

Figure 5.18: Employees in Department page

5.2.2.7 Admin Profile

Figure 5.19 displays the admin profile page that allows him to manage his account and personal information.

Features:

- Display admin information (name, email, and mobile number)
- Option to reset information
- Option to change password

Farah can manage her personal details on the profile page. She can view her account information like name, email, and mobile number. Farah can update her profile settings and click on reset information button or change her password and click change password button.

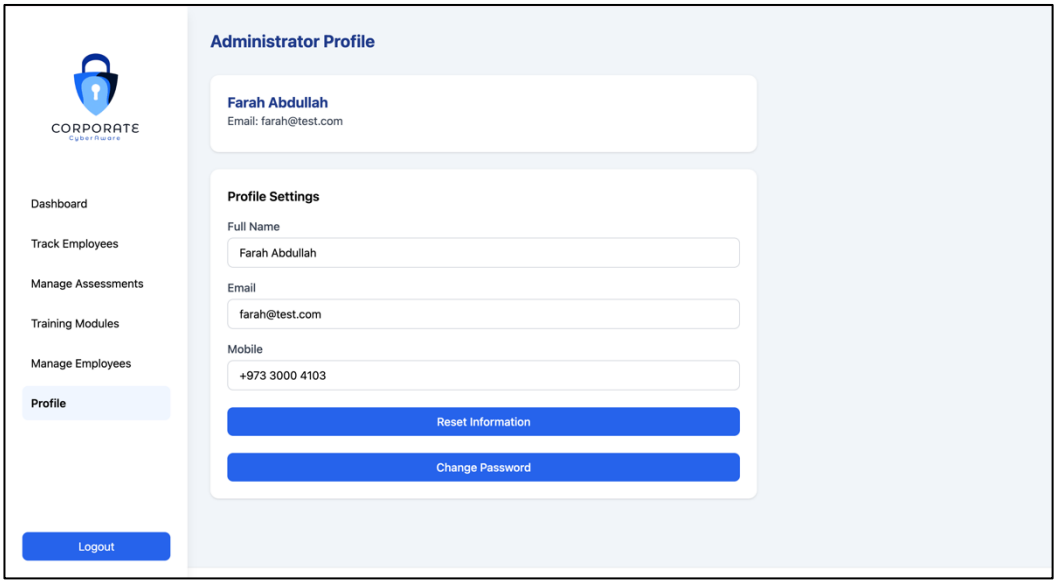

Figure 5.19: Admin Profile Page

5.3 Algorithm Design

CyberAware's main algorithms were designed to perform the system's core operations, including user authentication, assessment evaluation, phishing simulation handling, and risk analysis. This section presents algorithms' logic using pseudocode to describe and explain the system flow.

Algorithm 1: User Login and Authentication

```
INPUT: email, password
FETCH user FROM Employees WHERE email = input_email
IF user exists THEN
IF password matches stored password_hash THEN
IF role = admin THEN
redirect to admin dashboard
ELSE
redirect to employee dashboard
ENDIF
ELSE
display "InvYaqoobd password"
ENDIF
ELSE
display "User not found"
ENDIF
```

The user login algorithm manipulates user authentication and ensures secure role-based access to the system. First, it verifies whether the email is registered in the system, then it checks the

password using its hash value. After successfully verifying the email and password, it redirects the user to the appropriate dashboard (Admin or Employee).

Algorithm 2: Assessment Evaluation

```
INPUT: employee_id, assessment_id, answers[]
SET score = 0
FOR each question in assessment
     GET correct_option

    IF employee_answer == correct_option THEN
         score = score + 1
     ENDIF
ENDFOR

STORE score in Employee_Assessments
IF score >= passing_mark THEN
     set passed = TRUE
 ELSE
     set passed = FALSE
ENDIF
RETURN score
```

The evaluation algorithm calculates the employee's score after completing an assessment by comparing the user answer and the correct answer for each question and updates the score repeatedly. Then, it stores the final score in the database and determines if the employee passed or failed the assessment.

Algorithm 3: AI-Based Assessment Generation

```
INPUT: assessment_topic, difficulty_level, admin_prompt
ADMIN enters request into AI chatbot

SEND assessment_topic, difficulty_level, and admin_prompt to AI
Chatbase
RECEIVE generated_assessment_questions
DISPLAY generated_assessment_questions to admin
ADMIN copies selected questions
PASTE questions into assessment creation form
STORE assessment and questions in Assessments database
ASSIGN assessment to employees
WAIT for employee submission

STORE employee responses and scores in Assessment_Results
GENERATE performance insights and feedback
```

The AI-based assessment algorithm enables administrators to chat with the AI chatbot and request them to generate specified assessment questions based on a selected topic and difficulty level. The generated questions are reviewed by the admin, then the admin copy it into the form, and assigned to employees.

Algorithm 4: Risk Report Generation

```
INPUT: employee_id

FETCH assessment scores
FETCH simulation behavior

CALCULATE total_score

IF total_score >= 80% THEN
    risk_level = "low"
ELSE IF total_score >= 50% THEN
    risk_level = "medium"
ELSE
    risk_level = "high"
ENDIF

STORE result in Risk_Reports
```

The risk report generation algorithm helps administrators identify employees who may require additional cybersecurity training. It generates a risk report for each employee and categorizes them as high risk, medium risk, or low risk based on their assessment score and behavior.

Algorithm 5: Module Progress Tracking

```
INPUT: employee_id, module_id, completed_section

FETCH current progress FROM Employee_Modules

UPDATE progress based on completed_section

IF progress = 100% THEN
    status = "completed"
    SET completed_at = current timestamp
ELSE
    status = "in progress"
ENDIF

SAVE updated progress and status
```

The tracking algorithm provides real-time employee progress tracking to allow administrators to monitor employee engagement. So, each time an employee completes a section, the system updates the progress percentage. And once the progress reaches 100%, the module is marked as accomplished.

Chapter 6: System Implementation and Testing

6.0 Introduction

In this chapter, we will outline the testing and implementation of the corporate CyberAware system. The chapter dives into explaining the technologies, components, and technologies used to construct the system and how they are incorporated into a functioning prototype. Additionally, it presents the system workflow.

Furthermore, the chapter covers the evaluation and testing process used to make sure the system executes properly, securely, and efficiently. A selected number of testing methods including functional, security, and performance testing were conducted to examine the level of reliability and capability of the system. This chapter additionally explores the system's findings, strengths, and weaknesses.

6.1 System Implementation

6.1.1 Development Environment Table

Table 6.1 shows that Corporate CyberAware system was implemented using a variety of tools and technologies. These technologies were selected to support front-end development, back-end processing, database management, analytical visualization, API testing, and AI-based assessment and training module generation.

Components	Technology Used	Purpose
Frontend	HTML, Tailwind CSS, JavaScript	User Interface
Backend	Python, Flask	System Processing
Database	MySQL	Store System Data
Database Management	phpMyAdmin	Manage Database
API Testing	Postman	Test APIs
Code Editor	Visual Studio Code	Development
Charts	Chart.js	Analytics Visualization
AI Assistant	Chatbase AI	Generate assessments and training modules

Table 6.1: Development Environment and Technologies Used

6.1.2 System Integration

Corporate CyberAware integrates the front-end, back-end, database, analytics, and artificial intelligence components into a single web-based platform. Frontend interface was developed using HTML, Tailwind CSS, and JavaScript. To accomplish system tasks, the frontend communicates with the Flask APIs on the backend. MySQL is used as the backend for storing and retrieving data. AI was integrated to the system to generate assessments and training modules.

6.1.3 System Flow

6.1.3.1 Employee Workflow

An employee interacts with the Corporate CyberAware system by following these workflow steps to complete the desired tasks from him like answering assessments and viewing training modules.

1- Employee logs into the system using assigned credentials.
2- Employee access assigned assessments and training modules.
3- Employee answer assigned assessment questions.
4- Employee view assigned training modules.
5- Employee results are stored in the main database and shown to the employee in the dashboard.
6- The system generates behavioral insights based the employee performance.

6.1.3.2 Admin Workflow

The admin communicates with the Corporate CyberAware system by accomplishing a set of workflow steps to help him manage employees and view their progress alongside with the overall company's progress.

1- Admin sign-up in the system and creates an account.
2- Admin logs into the system with credentials.
3- Admin can manage organization's overall progress and track employees and departments.
4- Admin can create, edit, and assign cybersecurity assessments with the use of AI chat-bot.
5- Admin can create, edit, and assign training modules with the use of AI chat-bot.
6- Admin can track employee overall assessment performance and results.
7- Admin can generate assessment reports to track employee progress.

6.2 System Testing

6.2.1 Functional Testing

To verify the functionalities of the Corporate CyberAware system and ensure optimal operation according to the system requirements, functional testing was performed. The process of testing included checking user authentication, departments and employee management, assessment assignment, training modules, analytics, and reporting features. And to confirm appropriate system behavior testing was performed with different scenarios for both administrator and employee.

Testing Area	Target	Result	Explanation
Login Authentication	Login form	√	Users successfully logged in using correct credentials

Invalid Login Handling	Login form	√	System rejected invalid usernames and passwords and shows an alert
Add Employee	Employee management	√	Administrator successfully added employee to the department
Remove Employee	Employee management	√	Employee were deleted from department correctly
Create and remove Department	Department management	√	Department was created and deleted successfully
Create Assessment	Assessment module	√	Assessment was created and saved to the database correctly
Edit Assessment	Assessment module	√	Assessment updated successfully
Delete Assessment	Assessment module	√	Assessment was removed correctly
Submit Assessment	Assessment page	√	Employee answers were submitted and used for insights successfully
Score Calculation	Assessment system	√	System calculated assessment scores accurately and generate a report of it
Assign Training Modules	Training module system	√	Training module was assigned to the employees correctly
Dashboard Analytics	Dashboard	√	Charts and analytics updated immediately
Feedback Display	Analytics page	√	Personalized feedback displayed correctly for both admin and employee
Search and Filtering	Employee tracking	√	Search and filtering features worked appropriately
AI Assessment Generation	AI chatbot integration	√	AI chatbot worked well and generated assessments for the admin

Table 6.2: Functional testing areas and results

The result of the testing shows all main functionalities of Corporate CyberAware worked as intended without any issues. The system managed users' requests like database operations, assessment processing, and analytics generation correctly, which ensures that the system works as specified and planned.

6.2.2 Security Testing

6.2.2.1 SQL Injection Testing

Figure 6.1 shows the SQL Injection testing for Corporate CyberAware. Based on Figure X.X it shows that the system is secured from SQL Injection attack since the email input field did not accept entering ‘ or 1=1 – and validates the input.

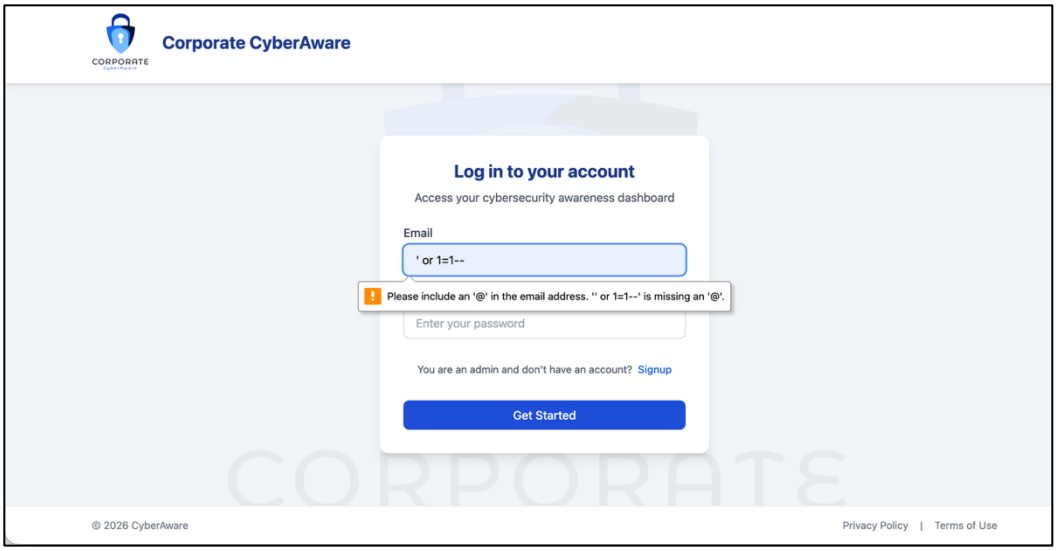

Figure 6.1: SQL Injection

6.2.2.2 XSS Testing

Based on Figure 6.2, the Corporate CyberAware system is secured against XSS attacks. The system did not response to malicious JavaScript code.

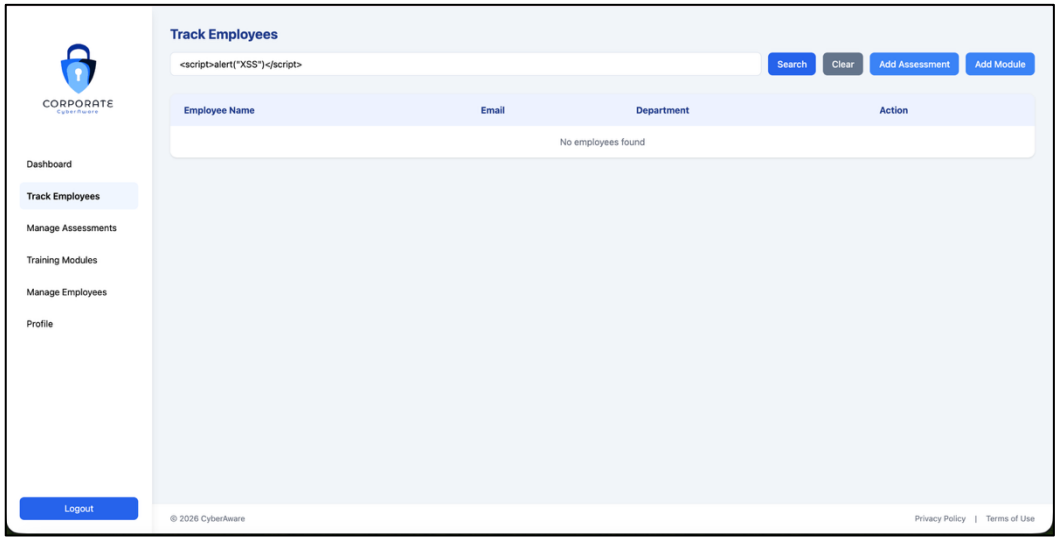

Figure 6.2: XSS Testing

6.2.2.3 Input Validation

Figure 6.3 shows that Corporate CyberAware system has input validation. It does not allow to enter other characters than letters in the Full Name field and only allow to enter email as shown in Figure 6.4. In addition, Corporate CyberAware system does not allow to change the drop-down list because it verifies the input using a whitelist.

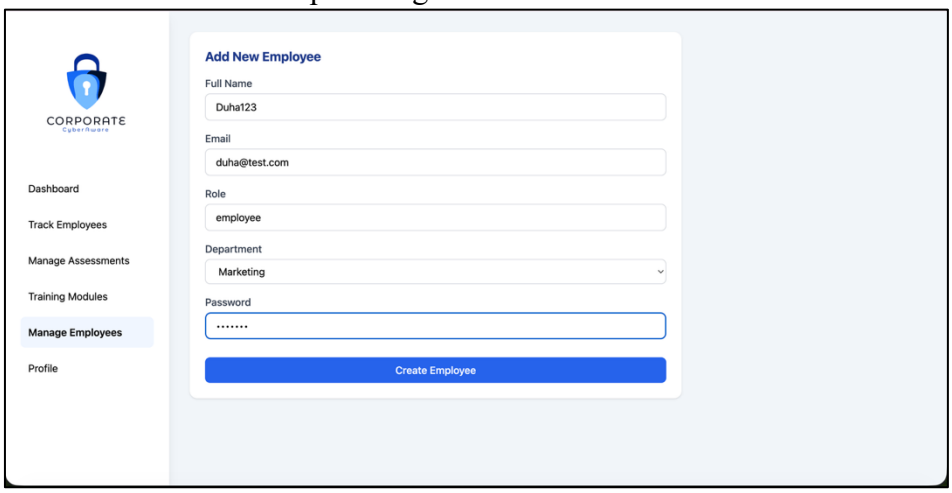

Figure 6.3: Input Validation

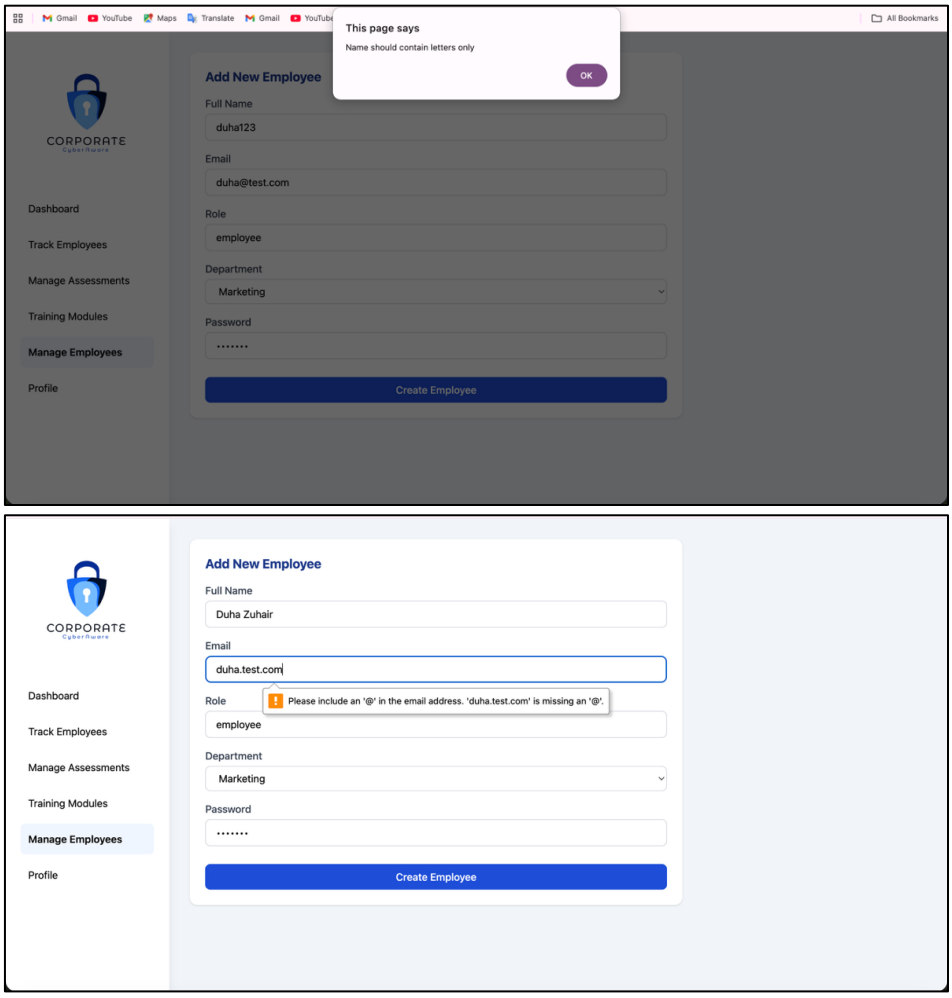

Figure 6.4: Name and Email Fields Validation Testing

6.2.3 Performance Testing

Testing the performance was conducted to measure the response time and effectiveness of the system during typical conditions. The performance testing process verified only key functions comprising login authentication, dashboard loading, assessment processing and scoring, and report and analytics generation. The testing environment hardware and software are presented in Table 6.3.

Component	Specification
Device	MacBook Air-2022
Processor	Apple M2
RAM	8 GB
Operating System	macOS Tahoe 26.3.1
Browser	Google Chrome

Table 6.3: Testing environment specifications

According to the obtained results, it showed that the system operated efficiently without delays, and the system is anticipated to support larger numbers of users while conserving reliable performance regarding the isolated architecture. The table 6.3 shows the recorded results using time feature in network tab.

Function	Response time
User login and authentication	0.8 seconds
Dashboard loading (both admin and employee)	1.2 seconds
Upload assessments for admin, and display at user screen	1.0 seconds
Submit assessment and scoring	1.6 seconds
Generate reports and feedback (both admin and employee)	2.1 seconds
Load analytics page	1.5 seconds

Table 6.4: System performance testing results (for key features)

6.2.4 Usability Testing

Six members with corporate backgrounds were involved in a focus group to provide feedback for usability testing for Corporate CyberAware. The main goal was to assess the ease, usability, and helpfulness of the system when executed in a real corporate setting.

Participants engaged with the system by executing simple tasks including accessing training materials, exploring the dashboard, and performing assessments. Participants were surveyed to provide feedback on their overall experience and thoughts on the system's usability, and clarity after using it.

Majority of the participants expressed satisfaction with the system's ease of use, clarity, and structure. They pointed out on how simple it is to use the dashboard and assessment tools and access training modules; it was helpful in comprehending cybersecurity performance. Nonetheless, few individuals proposed minor changes, such as short direction for new users. As a whole, the findings showed that the system is efficient and easy to use for corporates and businesses. The feedback obtained contains helpful information for improving the system's usability more effectively.

6.2.5 Comparison with chapter 2 frameworks

The Table 6,5 illustrates how our system Corporate CyberAware addresses deficiencies of current frameworks explained in chapter 2 as a comparison. The system provides behavior-based monitoring, ongoing feedback, and continuous awareness and training into a single fully integrated system.

Feature / Aspect	**CAT Framework**	**ICAT Model**	**ECAF Framework**	**Corporate CyberAware (Our System)**
Focus	Levels of understanding and knowledge	Flexible engagement and training	Cognitive and behavioral aspects	Ongoing assessment evaluation and development
Type of assessment	Questionnaires	Regular assessments	Reports and assessments	Custom assessments, according to performance
Adaptability	Non-adaptive and fixed	Flexible training	Limited adaptability	Flexible Adaptable and continuously revised
Feedback Mechanism	minimal feedback	Adaptable feedback	Conceptual feedback	Ongoing feedback and insights

Behavioral Monitoring	Not incorporated	Supported partly	Limited (psychological only)	Completely supported (tracking based on performance)
Practical Implementation	Static and conceptual	Practical in part	Based on research and theoretical	Completely functional web-based system
Customization	General to all users	Customized in part	Based on profiling	Completely customized for staff
Continuous Assessment	Not incorporated	Constrained (periodic)	Not incorporated fully	Completely continuous observation and assessment

Table6.5: Comparison with existing frameworks

6.2.6 Strengths and Weaknesses

Our system, Corporate CyberAware, provides several strengths that contribute to the effectiveness of increasing cybersecurity awareness in corporates. The strengths include a user-friendly interface that enables users (admin or employee) to navigate easily and a behavioral-based assessment evaluation to analyze employees' cybersecurity awareness that goes beyond academic knowledge. In addition, the system supports ongoing employee performance monitoring through regular training and assessments, identifies the organization's required improvements and weak areas to help enhance its overall awareness, provides analytics and generates reports to help admins track employees and assist in decision-making, and offers a seamless integration of analytics, dashboard, management, and reporting to also help in understanding behavioral trends and enhancing overall awareness.

Despite our system's strengths, it also comes with several weaknesses. These weaknesses include the system not being fully deployed in a real organizational environment which restricts its validation in a real-world situation; the limited implementation of advanced AI technologies for automated suggestions and predictive analysis; the system being web-based, there is a huge dependence on a reliable internet connection which affects its availability in the absence of internet; scalability and performance under high load are impacted since the system is not tested on a large number of users; and some of the features, such as report customization, still being limited and in need of improvement in future developments.

Chapter 7: Conclusion and future work

7.0 Conclusion

This project identified the effect of user behavior on cybersecurity incidents, especially among employees within organizations. The performed literature review and requirement analysis clearly showed that existing cybersecurity awareness approaches are restricted in their assessment of user behavior and reliance on one-time generic training sessions.

In order to resolve these limitations, this project designed a behavior-oriented web-based cybersecurity awareness and assessment system, Corporate CyberAware. The system emphasizes continuous evaluation of employees' awareness through assessments, phishing simulations, and behavioral analysis. In addition to real-time feedback reports and customized training suggestions.

The system architecture involves several components consisting of assessment management, training modules, performance tracking, and risk reporting, all backed with an organized database and simple user interfaces for both administrators and employees. Furthermore, the use of a recursive Agile development approach-maintained versatility and ongoing improvement throughout the project lifecycle.

Generally, Corporate CyberAware enhances the overall organizational cybersecurity level by switching static awareness into a continuous behavioral improvement process. It illustrates how cybersecurity awareness can be evaluated, monitored, and improved to reduce human-related cyber risks.

7.1 Future Work

Although Corporate CyberAware delivers a thorough solution to assess and enhance employees' cybersecurity awareness, there are still certain improvements to be premeditated for future development.

First, the system can deliver an additional effective customized experience by incorporating artificial intelligence techniques to automatically generate tailored training suggestions based on the employee's behavior without the intervention of the administrator.

Second, the phishing simulation part can be extended to provide further realistic evaluation by integrating practical email-based simulations within organizational environments.

Another promising improvement is developing an application version of the system to steer within organizational environments and increase employees' engagement.

Additionally, future work may increase administrators' productivity by enabling the upload of external assessment materials. It would provide a diversity of learning content and support emerging threats.

Eventually, implementing and evaluating the system within a real organization would provide an accurate perception of the system's functionality and effectiveness, enabling profound refinement based on real feedback.

References

Bishop, L., Asquith, P. & Morgan, P., 2025. The Employee Cybersecurity Awareness Framework. *Human Behavior and Emerging Technologies,* Volume 2025, p. 24.

Donekal Chandrashekar, N., Lee, A., Azab, M. & Gracanin, D., 2024. Understanding user behavior for enhancing cybersecurity training with immersive gamified platforms. *Information,* 15(12), p. 814.

Hijji, M. & Alam, G., 2022. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors,* Volume 22.

National Cyber Security Center, n.d. *Industrial Control Systems.* [Online]
Available at: https://www.ncsc.gov.bh/en/cyberwiser/ics.html
[Accessed 1 February 2026].

Pothu, A. R., 2025. Behavioural Analysis of End-Users for Enhancing Cybersecurity Awareness and Prevention. *AVE Trends in Intelligent Computer Letters,* 1(1), pp. 31-40.

Quchi, M. M., Hakimi, M. & Fazil, A. W., 2024. Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID),* 3(1), p. 20–33.

Saif Al-Dean Qawasme, A. A. S. A. M. K. K., 2025. Navigating cybersecurity training: A comprehensive review. *Computers and Electrical Engineering.*

Shaik Mohammed Junaid, J. J. S. S. P. C. G., 2025. *Design and Implementation of an Interactive Web- Based Cybersecurity Awareness Training Platform with Role-Based Personalization and Threat Simulation.* s.l., IEEE.

Shouq Alrobaian, S. A. A. A., 2023. Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation. *Big Data and Cognitive Computing,* 7(2), p. 73.

Taherdoost, H., 2024. Towards an Innovative Model for Cybersecurity Awareness Training. *information,* Volume 15.

The Daily Tribune - News Of Bahrain, 2022. *Cyber Attacks In Bahrain Have Sky-Rocketed, Say Experts.* [Online]
Available at: https://www.newsofbahrain.com/bahrain/83046.html
[Accessed 1 February 2026].

Ünsal, N. Ö. & Ocak, M. A., 2026. Development of Organizational Cybersecurity Awareness Scale (OCAS). *Hacettepe University Journal of Education ,* 41(1), p. 136–155.

Ussher-Eke, D., 2025. From awareness to action: Designing effective cybersecurity training programs. *International Journal of Science and Research Archive,* 16(02).