CSC 106 - Software Engineering 1

Section ABD1

**Final Term Project**



Submitted by:  
Angelica Lomarda

Erol Daguinod

Leamie Domingo

Submitted to:

*Mr. Klinth Jerald L. Matugas*

DECEMBER 2025

# TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_heading=h.i1jpvspr5c8n)

[1.1. Team & Contacts 3](#_heading=h.1jnddll1yml1)

[1.2. Executive Summary 3](#_heading=h.gkmgydqtp6zl)

[1.3. Problem Statement 3](#_heading=h.81m9aida1fw1)

[1.4. Project Goals & Objectives 3](#_heading=h.6my1s6af5tby)

[1.5. Scope & Limitations 4](#_heading=h.dtps1ulucdgv)

[2. Related Review of Literature 4](#_heading=h.casjtgnuxb3k)

[2.1. Related Work & Technologies 4](#_heading=h.47uk3eyp3pbx)

[2.2. Domain Analysis 4](#_heading=h.a6og17derktb)

[3. Project Methodology 4](#_heading=h.qu159d4m0rn6)

[3.1. Development Process 4](#_heading=h.6kkxtahhliuy)

[3.2. Timeline & Milestones 5](#_heading=h.9isnepide4ni)

[3.3. Stakeholder Analysis 5](#_heading=h.f7tud7tj14df)

[3.4. Initial Requirements Gathering 5](#_heading=h.42hizpibdxhi)

[4. System Specification 5](#_heading=h.c20qf84sxpkh)

[4.1. User Personas & Stories 5](#_heading=h.kqi1e3eujshi)

[4.2. Functional Requirements 5](#_heading=h.ixiu3pavaixk)

[4.3. Non-Functional Requirements (NFRs) 6](#_heading=h.9e7om96o5bs3)

[4.4. System Architecture & Design 6](#_heading=h.lvhrwrsny5uc)

[5. Feasibility & Risk Analysis 6](#_heading=h.84crx584vb9)

[5.1. Technical Feasibility 6](#_heading=h.moi5cqr6oq9j)

[5.2. Risk Register 7](#_heading=h.8g0hh6w4om2s)

[6. Testing, Validation & Deployment 7](#_heading=h.osc9vgcreaqr)

[6.1. Test Strategy 7](#_heading=h.rnfeh8vh8fy3)

[6.2. User Validation Plan 7](#_heading=h.ckaskpftfhkp)

[6.3. Deployment Plan 7](#_heading=h.no9jsw7br8o)

[7. Conclusion & Future Work 8](#_heading=h.2jrc5z3ju0u5)

[8. References 8](#_heading=h.tnyy9lz1mqy6)

[9. Appendices 8](#_heading=h.q0z6g2y5x4ls)

# 1. Project Overview

### 1.1. Team & Contacts

| **Role** | **Name** | **Responsibilities** | **Contact** |
| --- | --- | --- | --- |
| **Project Manager** | Erol Daguinod | Oversees project timeline, scope, and stakeholder communication. | daguinoderol33@gmail.com |
| **Technical Lead** | Erol Daguinod | Leads system architecture, core development, and technical decisions. | daguinoderol33@gmail.com |
| **UI/UX Designer** | Angelica Lomarda | Designs user interfaces, prototypes, and ensures a positive user experience. | lomarda.angelica4505@gmail.com |
| **QA Lead** | Leamie Domingo | Develops test plans, ensures software quality and functionality. | leamiedomingo@gmail.com |

### 1.2. Executive Summary

The Secure Pass Portal is a web-based system designed for Philmen’s Credit Corporation under the Romarate Group of Companies. The system improves security, supports employee authentication, keeps the transactions secure, and reduces system issues identified during data gathering. Built using Laravel, it provides secure login, role-based access, and session management for reliable and controlled access.

### 1.3. Problem Statement

**Current Situation:**

Employees of Philmen’s Credit Corporation rely on an existing system that experiences login difficulties, occasional downtime, and inconsistent access control. Users often encounter delays when accessing the system, especially during peak working hours, and administrators have limited visibility over user activity and security threats.

**Pain Points:**

* Difficulty logging in due to system errors or forgotten credentials
* Security concerns such as unauthorized access and potential hacking attempts
* Data inconsistencies caused by system synchronization issues
* Manual processes for account recovery and system maintenance
* Steep learning curve requiring frequent employee training

**Impact:**

These issues lead to reduced employee productivity, delayed transactions, increased workload for administrators, and user frustration. Security risks also expose the organization to potential data breaches and compliance problems, affecting overall system reliability and trust.

### 1.4. Project Goals & Objectives

*List the primary goals and specific, measurable objectives. Use the SMART (Specific, Measurable, Achievable, Relevant, Time-bound) framework where possible.*

* **Goal 1:** Improve system security
  + **Objective 1.1:** Implement secure authentication
  + **Objective 1.2:** Apply role-based access for administrators and employees
* **Goal 2:** Enhance system usability
  + **Objective 2.1:** Reduce login errors
  + **Objective 2.2:** Provide password reset and email verification

### 1.5. Scope & Limitations

| **Category** | **Description** |
| --- | --- |
| **In Scope** | • *Features:* Secure login and authentication, user registration, email verification, password reset, role-based access control, session management, and logout functionality. • *User Base:* Primary users are Philmen’s Credit Corporation employees. Secondary users are system administrators responsible for access control and monitoring.  • *Data Sources:* User-provided credentials (username, password), email addresses for verification, and stored user records in the database. |
| **Out of Scope** | • Full company system integration  • Mobile version  • Financial processing modules |
| **Constraints & Limitations** | • *Technical:* The system is built using the Laravel framework and relies on email services for verification and password recovery, which may be subject to delivery delays.  • *Assumptions:* Users provide accurate registration details and have access to valid email accounts. • *Known Issues:* The system has not undergone large-scale performance testing and is evaluated based on a limited number of users. |

# 2. Related Review of Literature

### 2.1. Related Work & Technologies

Existing authentication and access control systems are widely used in web applications to protect sensitive data and ensure authorized system access. Common solutions include framework-built authentication modules, enterprise login systems, and custom-developed portals. These systems informed the design and implementation of the Secure Pass Portal.

* **Competitive Analysis:**
  + **Existing Tool 1:** Default Laravel Authentication (Jetstream / Breeze)
    - Strengths:
      * Built-in authentication features such as login, registration, password reset, and email verification
      * Secure password hashing and middleware protection
      * Well-documented and actively maintained
    - Weaknesses:
      * Generic user flow that may not fit specific company roles
      * Requires customization for organization-specific access control
  + **Existing Tool 2:** Manual Username–Password Systems
    - Strengths:
      * Simple to implement
      * Minimal system requirements
    - Weaknesses:
      * Higher risk of security vulnerabilities
      * Poor user experience due to lack of recovery and monitoring features
  + **Existing Tool 3: Centralized Enterprise Login Systems**
    - *Strengths:*
      * High-level security and centralized management
      * Supports logging and monitoring
    - *Weaknesses:*
      * Expensive to deploy and maintain
      * Overly complex for small-to-medium organizations

The Secure Pass Portal improves on these systems by providing a lightweight, role-based authentication solution tailored specifically to Philmen’s Credit Corporation without the complexity and cost of enterprise platforms.

* **Technology Stack Rationale:**

The Secure Pass Portal is developed using the following technologies:

* **Programming Language:** PHP, chosen for its reliability and wide use in web development
* **Framework:** Laravel, selected for its built-in security features, MVC architecture, and rapid development support
* **Database:** MySQL, used for secure and structured storage of user data
* **Security Tools:** Laravel’s password hashing, middleware, and session handling mechanisms
* **Email Services:** Used for account verification and password recovery

This technology stack enables rapid development, strong security, and maintainability while remaining cost-effective and suitable for the organization’s needs.

### 2.2. Domain Analysis

Authentication and access control systems are critical components of information security, particularly in organizational web applications. Research emphasizes that weak authentication mechanisms are among the leading causes of data breaches and unauthorized system access (Stallings, 2018). Effective login systems should incorporate secure credential handling, session management, and role-based access control to minimize security risks (Behl & Behl, 2020).

Studies also highlight that usability plays a significant role in authentication systems. According to Nielsen (2012), overly complex login procedures increase user error rates and frustration, which can lead to unsafe practices such as password reuse and sharing. Web frameworks that integrate security and usability features can reduce these issues by standardizing authentication processes (Laravel Documentation, 2024).

* **Key Findings:**

Existing literature indicates that secure authentication systems must balance security and usability. Strong password hashing, email verification, and controlled access are essential security features, while clear error handling and recovery options improve user experience (Stallings, 2018; Nielsen, 2012).

* **Gap Identification:**

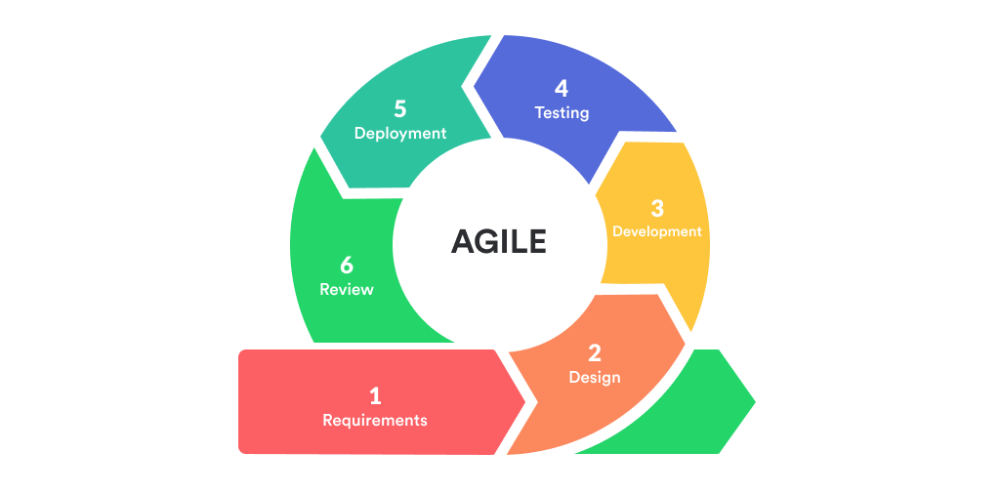
While many authentication solutions focus heavily on security or are embedded into large enterprise systems, there is a lack of lightweight, role-specific authentication portals tailored for small-to-medium organizations. The Secure Pass Portal addresses this gap by providing a secure, user-friendly, and customizable authentication system designed specifically for Philmen’s Credit Corporation, without the complexity or cost of enterprise-level solutions.

# 3. Project Methodology

### 3.1. Development Process

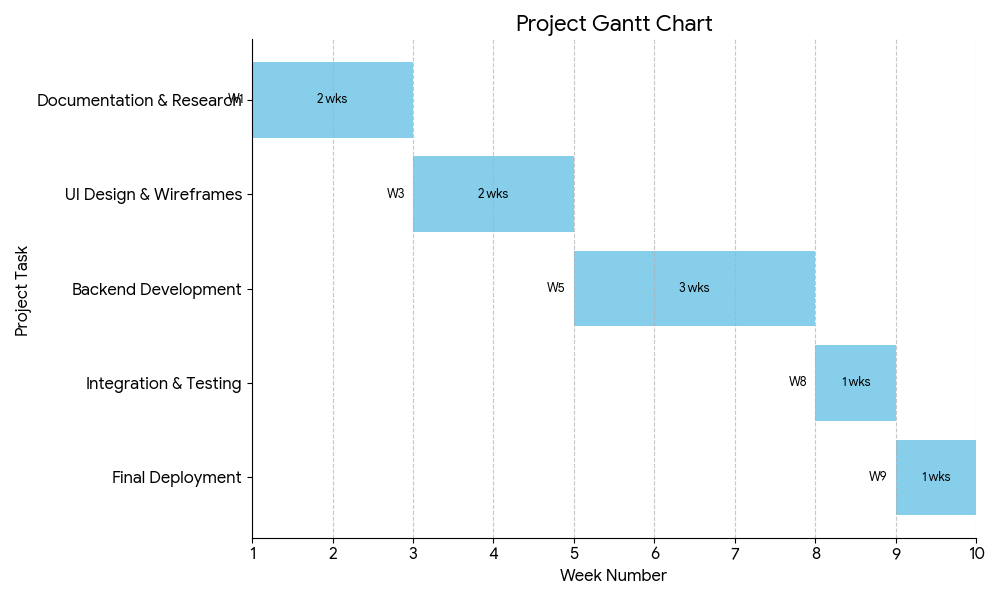
The project uses Agile/Scrum for iterative development and continuous feedback. Each sprint lasts two weeks, with sprint planning, daily standups, sprint reviews, and retrospectives.

**Figure 3.1:** Agile/Scrum Development Model

  
Agile allows incremental delivery of features, early testing, and stakeholder feedback.

### 3.2. Timeline & Milestones

**Figure 3.2:** Project Timeline & Key Milestones



The visualization provided is a **Gantt Chart**, a project management tool used to illustrate a project schedule. It breaks down the entire project into sequential tasks and displays the timeline for each one.

**3.3. Stakeholder Analysis**

This section identifies the individuals and groups that have an interest in the Secure Pass Portal and describes their level of influence and involvement in the project.

* **Primary Stakeholders:**
  + **Philmen’s Employees (End-Users):** Daily users of the system for secure access to company resources. They have high interest in system usability and reliability but medium influence over design decisions.
  + **System Administrators (Philmen IT Team):** Responsible for managing user accounts, security, and system monitoring. They have high interest and high influence on system requirements and implementation.
  + **Project Sponsors / Management:** Ensure the system aligns with organizational goals and compliance requirements. They have high influence and high interest in project outcomes.
* **Secondary Stakeholders:**
  + **University / Instructor:** Oversees academic requirements, evaluates documentation and system implementation. Has medium influence and medium interest.
  + **Future Maintenance Team:** Will support and maintain the system after deployment. Has medium interest and medium influence on long-term sustainability.
* **Influence & Interest:**

Primary stakeholders directly affect system requirements and usage, requiring close collaboration throughout development. Secondary stakeholders provide guidance, evaluation, and long-term support, influencing future enhancements and maintenance decisions.

### 3.4. Initial Requirements Gathering

Initial system requirements were gathered through a structured survey administered to two employees working in financial institutions. The survey consisted of multiple-choice questions and follow-up open-ended questions focusing on system downtime, transaction processing, security, compliance, usability, and upgrade plans. The goal was to understand real user experiences and identify system-related challenges that could be addressed through improvement of authentication and access control.

**Figure 3.3:** Key Insight from Initial Survey  
Survey responses from two financial institution employees indicate that system integration issues and security concerns are the most significant challenges, shaping the need for a secure and reliable access control system.

# 4. System Specification

### 4.1. User Personas & Stories

**Persona 1: System Administrator**

* **Name:** Josephine Peling
* **Age:** 38
* **Position:** IT/System Administrator at Philmen’s Credit Corporation
* **Background:** Responsible for managing system access, monitoring security, and ensuring system reliability. Experienced in handling employee accounts and resolving access-related issues.
* **Goals:** Maintain secure access, prevent unauthorized login attempts, and monitor system activity.
* **Challenges:** Detecting security threats, managing multiple user accounts, and responding quickly to access issues.

**Persona 2: Employee User**

* **Name:** Dante Bustamante
* **Age:** 28
* **Position:** Customer Service Staff
* **Background:** Uses the system daily to access work-related tools and information. Has basic technical skills and depends on smooth system access during office hours.
* **Goals:** Log in quickly, recover forgotten passwords easily, and access features based on assigned roles.
* **Challenges:** Forgotten passwords, occasional login errors, and delays caused by system access issues.

#### **User Stories**

* As an Administrator, I want to manage user accounts, so that I can control system access and maintain security.
* As an Administrator, I want to monitor login activity, so that I can identify unauthorized access attempts.
* As an Employee, I want to log in using secure credentials, so that I can access my work dashboard efficiently.
* As an Employee, I want to reset my password easily, so that I can continue working without delays.
* As an Employee, I want to verify my email during registration, so that my account is secure and properly activated.

### 4.2. Functional Requirements

| **ID** | **Feature / Module** | **Description** |
| --- | --- | --- |
| **FR-1** | **User Authentication** | The system shall allow users to register and log in securely. |
| **FR-2** | **Role-Based Access** | The system shall redirect users to dashboards based on their assigned role. |
| **FR-3** | **Registration** | The system shall enable new users to create accounts. |
| **FR-4** | **Email Verification** | Accounts shall require verified emails to activate fully. |
| **FR-5** | **Password Reset** | Users shall be able to recover forgotten passwords securely. |
| **FR-6** | **Session Management** | The system shall maintain secure user sessions and allow proper logout. |

### 

### 4.3. Non-Functional Requirements (NFRs)

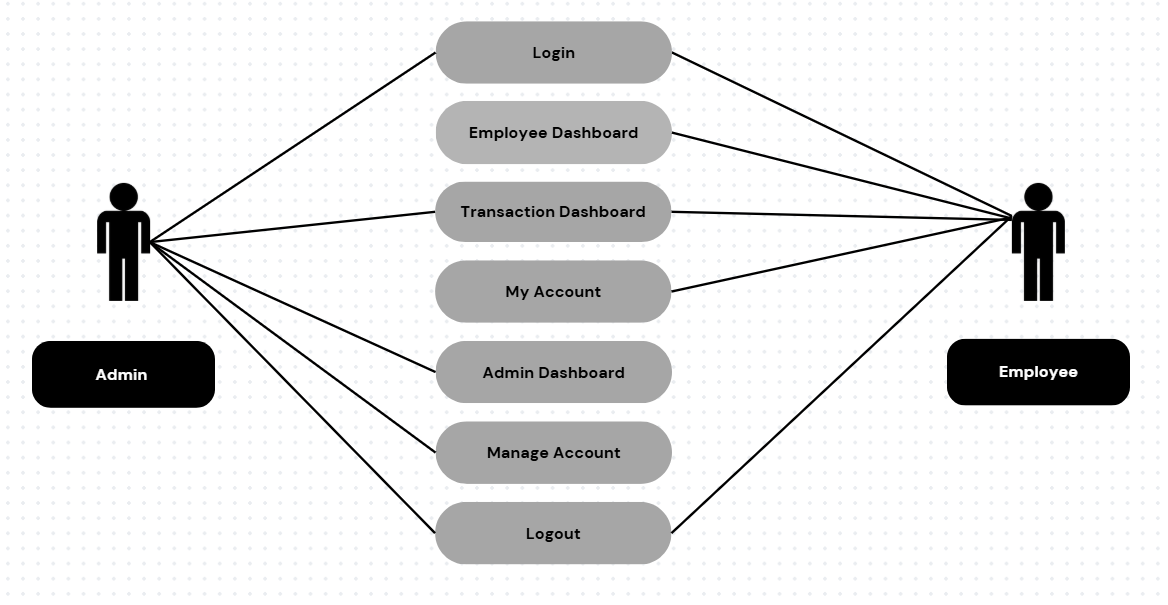
| **Category** | **Requirement** |
| --- | --- |
| **Performance** | • The system shall process login requests within 2 seconds.  • Role-based dashboard loading shall complete within 3 seconds. |
| **Usability** | • The system shall be intuitive for employees and administrators to use with less than 15 minutes of training.  • Error messages shall be clear and provide guidance for corrective action. |
| **Reliability** | • The system shall have 99.9% uptime during business hours.  • Automated backups shall be performed daily to prevent data loss. |
| **Security** | • All user credentials shall be hashed and stored securely.  • Data transmitted between the client and server shall be encrypted using HTTPS.  • Role-based access control shall restrict users to only permitted features. |

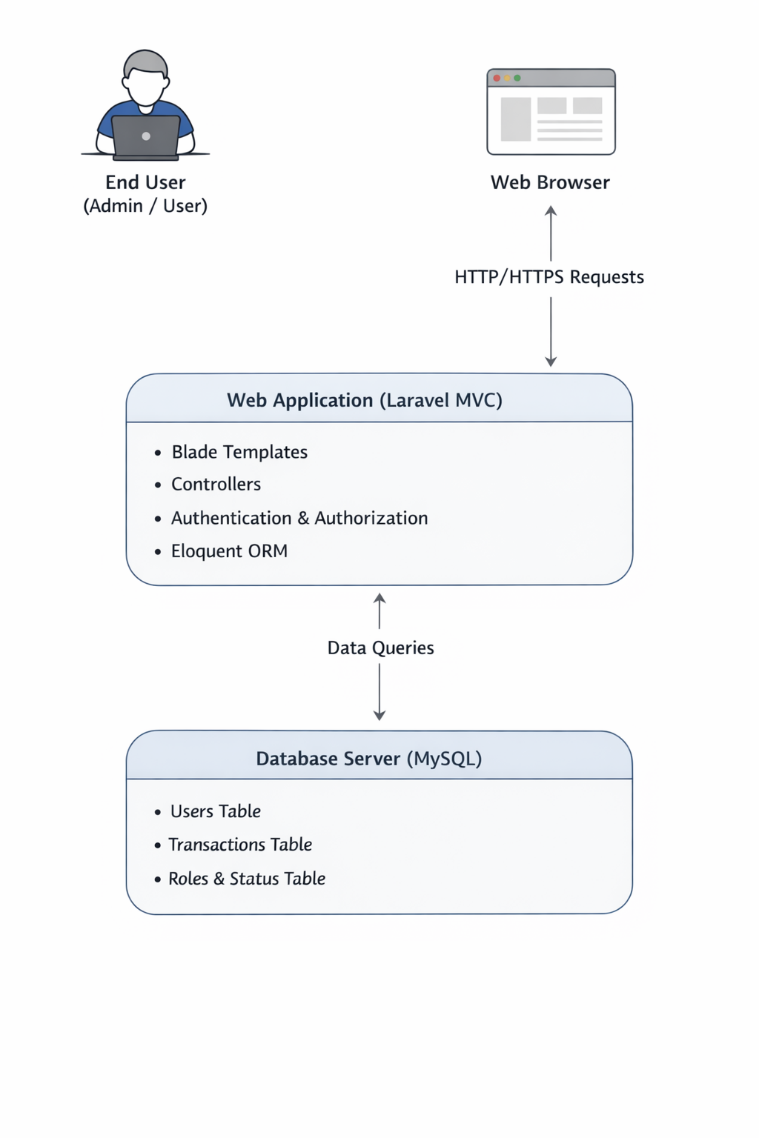
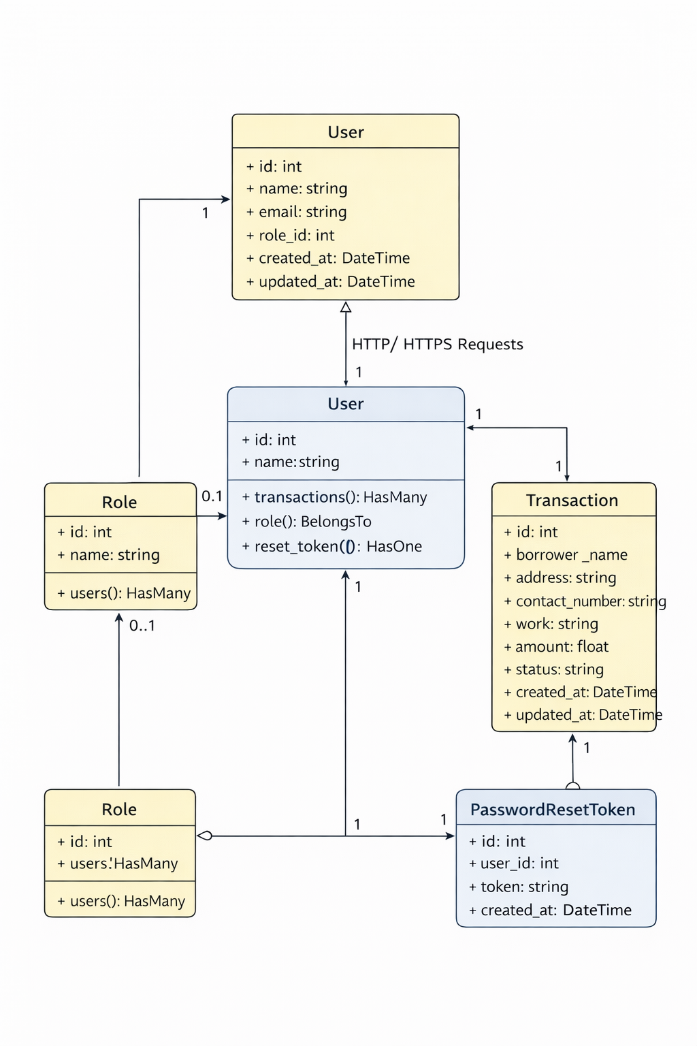
### 

### 4.4. System Architecture & Design

*.*

* **4.4.1. Use Case Diagram:**



* **4.2.2. System Architecture Diagram**
* **4.4.3. Class Diagram:**
* **4.4.4. Entity-Relationship Diagram (ERD):**

# 5. Feasibility & Risk Analysis

### 5.1. Technical Feasibility

* **Technology Maturity:** Laravel and MySQL are stable, well-documented, and industry standard.
* **Team Skills:** Members have foundational programming and web development experience. Tutorials/labs supported learning.
* **Proof of Concept:** Login prototype successfully built during Sprint 2, confirming technical viability.

### 5.2. Risk Register

| **Risk ID** | **Description** | **Probability** | **Impact** | **Mitigation Strategy** |
| --- | --- | --- | --- | --- |
| **R-1** | Email verification delays | Medium | Medium | Use reliable SMTP, add resend option |
| **R-2** | Role misconfiguration | Low | High | Add admin audit logs & testing |
| **R‑3** | Server downtime | Low | High | Enable backups & monitoring |

# 6. Testing, Validation & Deployment

### 6.1. Test Strategy

* **Unit Testing:** Laravel PHPUnit tests for authentication logic
* **Integration Testing:** Tests for registration-to-login workflow
* **User Acceptance Testing (UAT):** Employees test password reset, login speed, and usability

### 6.2. User Validation Plan

* **Method:**
* Participants will be asked to perform predefined tasks within the system while observers record their interactions, difficulties, and feedback. This allows the identification of interface or workflow issues that may affect user experience.
* Users will complete specific tasks, such as:
* Registering as a new user
* Adding a borrower
* Updating transaction status
* Resetting a password
* Performance, errors, and completion time will be recorded to evaluate system effectiveness and efficiency.
* **Success Criteria:**
* 90% of participants must complete login tasks without assistance
* System function tests pass with no critical issues
* Mean score ≥ 4.0 on usability questions
* **Likert Scale Interpretation:**

|  |  |
| --- | --- |
| **SCALE** | **VERBAL INTERPRETATION** |
| 5 | Strongly Agree |
| 4 | Agree |
| 3 | Neutral / Undecided |
| 2 | Disagree |
| 1 | Strongly Disagree |

### 

### 6.3. Deployment Plan

* **Environment:** The system is a web-based application developed using the Laravel framework and deployed on a cloud-hosted environment. It runs on a Linux-based server with a web server (Apache or Nginx), PHP runtime, and a MySQL database for data persistence. During development and testing, the application is hosted locally using tools such as Laragon, while production deployment is intended for a cloud platform (e.g., AWS, Heroku, or similar cloud hosting services) to ensure accessibility, scalability, and reliability.
* **Process:** The deployment process follows a controlled release workflow. Source code changes are maintained in a version control system (e.g., Git), with updates pushed to a main branch after testing. Deployment to the production environment is performed manually to ensure stability, allowing verification of system functionality before release. This approach minimizes deployment risks and ensures that only validated features are published to the live system.

# 7. Conclusion & Future Work

The Secure Pass Portal successfully improves login reliability, security, and usability tailored for Philmen’s Credit Corporation. It addresses current system issues and provides measurable improvements in authentication and access control.

* **V2.0 Features:**

### Future Work

* Mobile app version
* Multi-factor authentication (OTP)
* Admin analytics dashboard
* Audit logs and monitoring
* Single sign-on (SSO)
* Integration with full company system
* Performance testing for large-scale use

# 8. References

1. Laravel Documentation. (2024). Authentication. https://laravel.com/docs/10.x/authentication
2. Allafi, R., & Darem, A. A. D. (2025). Balancing usability and security in web applications. International Journal of Advanced and Applied Sciences, 12(6), 1–12. :contentReference[oaicite:3]{index=3}
3. Hof, H.-J. (2015). User‑centric IT security: How to design usable security mechanisms (arXiv:1506.07167). arXiv. :contentReference[oaicite:4]{index=4}
4. Usability of web authentication systems. (n.d.). In Wikipedia. Retrieved December 23, 2025, from https://en.wikipedia.org/wiki/Usability\_of\_web\_authentication\_systems :contentReference[oaicite:5]{index=5}
5. ISO 9241‑11:2018. (2018). Ergonomics of human‑system interaction — Part 11: Usability: Definitions and concepts. International Organization for Standardization.

# 9. Appendices

* **Appendix A:** Full Survey Questions and Raw Data

This survey aims to understand the current state of system problems within this financial institution, focusing on aspects like system downtime, impact on operations, security concerns, user experience, maintenance, backup/recovery, compliance, and plans for improvement. Your input will help identify key challenges and potential areas for enhancement in financial systems. Responses are for informational purposes to guide understanding and potential improvements in managing system-related issues in financial institutions.

**1. How often do you experience system downtime in critical financial operations?**

A. Rarely

B. Occasionally

C. Frequently

D. Almost daily

**2. How much do system problems impact daily financial operations?**

A. Minimal impact

B. Some impact

C. Significant impact

D. Severe impact affecting transactions/customers

**3. What’s the biggest system-related challenge in your financial institution?**

A. Security vulnerabilities

B. Slow processing speeds

C. Integration issues between systems

D. Downtime/failures

E. Other (please specify)

**4. Do you experience issues with transaction processing accuracy or speed?**

A. Rarely

B. Occasionally

C. Frequently

D. Constantly

**5. How concerned are you about system security in your financial institution?**

A. Not concerned

B. Slightly concerned

C. Moderately concerned

D. Very concerned

**6. How do employees generally find using the financial systems?**

A. Very user-friendly

B. Mostly okay

C. Some frustrations

D. Often difficult

**7. How often are financial systems updated or maintained?**

A. Regularly scheduled updates

B. Occasionally as needed

C. Rarely

D. We struggle to keep up with updates

**8. How confident are you in data backup and recovery processes for financial data?**

A. Very confident

B. Somewhat confident

C. Not very confident

D. Not confident at all

**9. Do system issues ever impact compliance with financial regulations?**

A. Never

B. Rarely

C. Occasionally

D. Frequently

**10. Are there plans to improve or upgrade financial systems in the near future?**

A. Yes, actively planning

B. Considering options

C. No immediate plans

D. Budget constraints limit upgrades

**Follow-up Questions:**

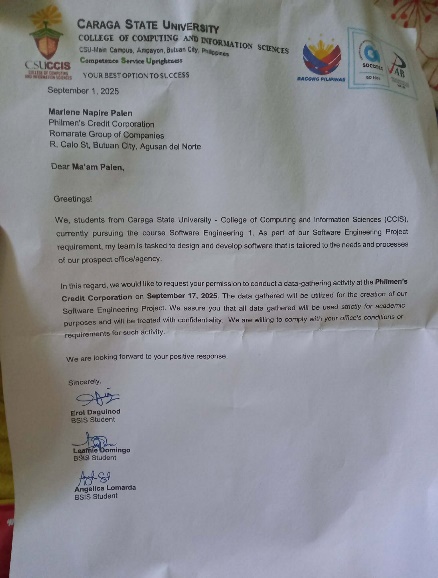
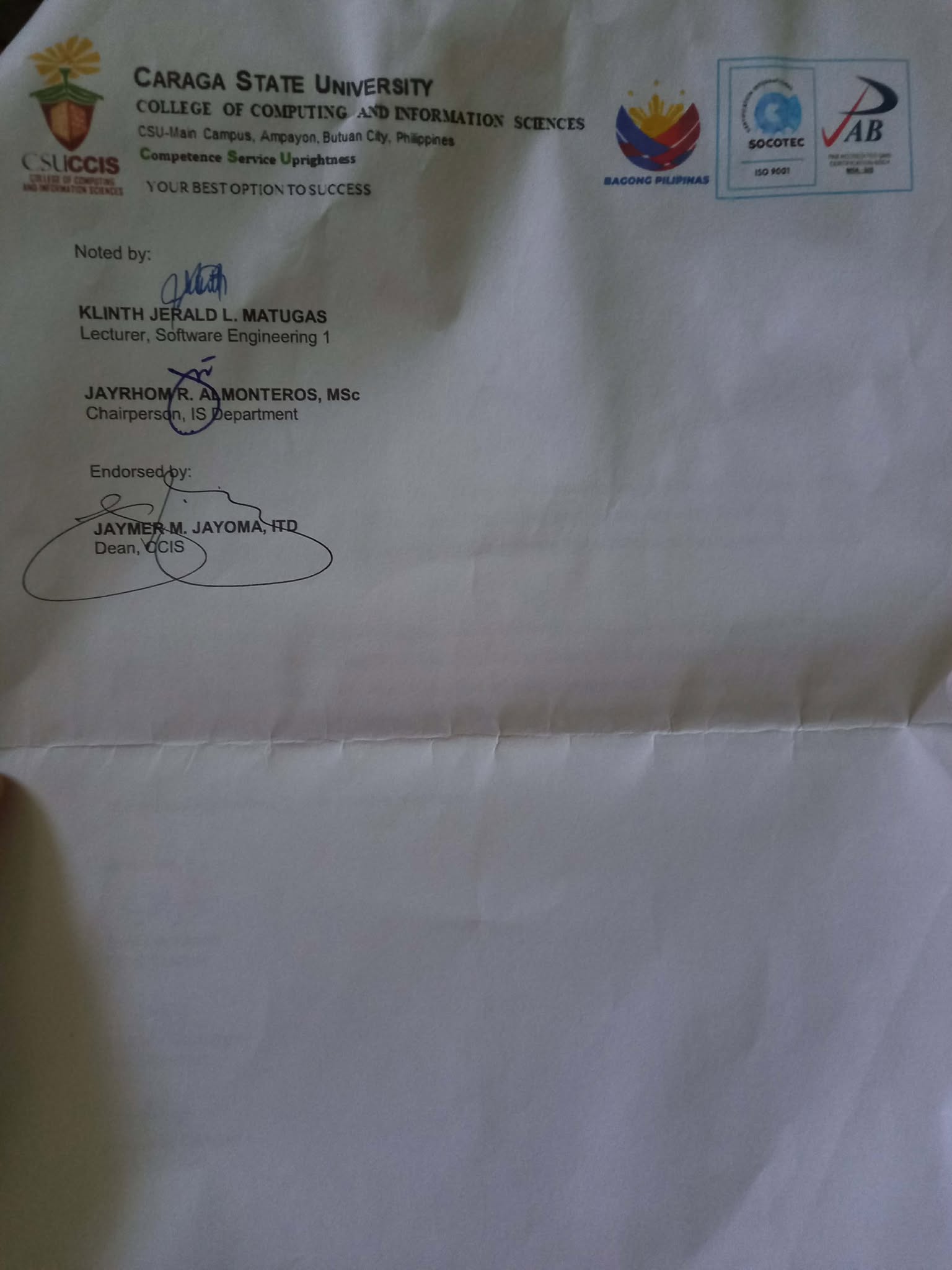
1. If you experience system downtime or issues, what are the typical impacts on financial operations?

2. What measures are in place to protect against security vulnerabilities in financial systems?

3. How do you ensure financial systems stay compliant with changing regulations?

4. What are the main drivers for considering system upgrades or improvements in your financial institution?

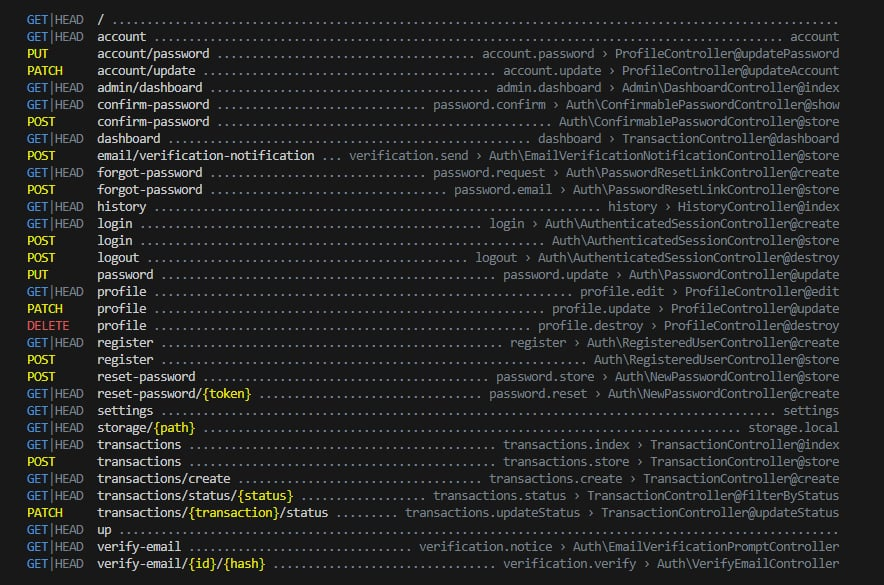
5. How are employees trained on using financial systems, and how often is refresher training done?

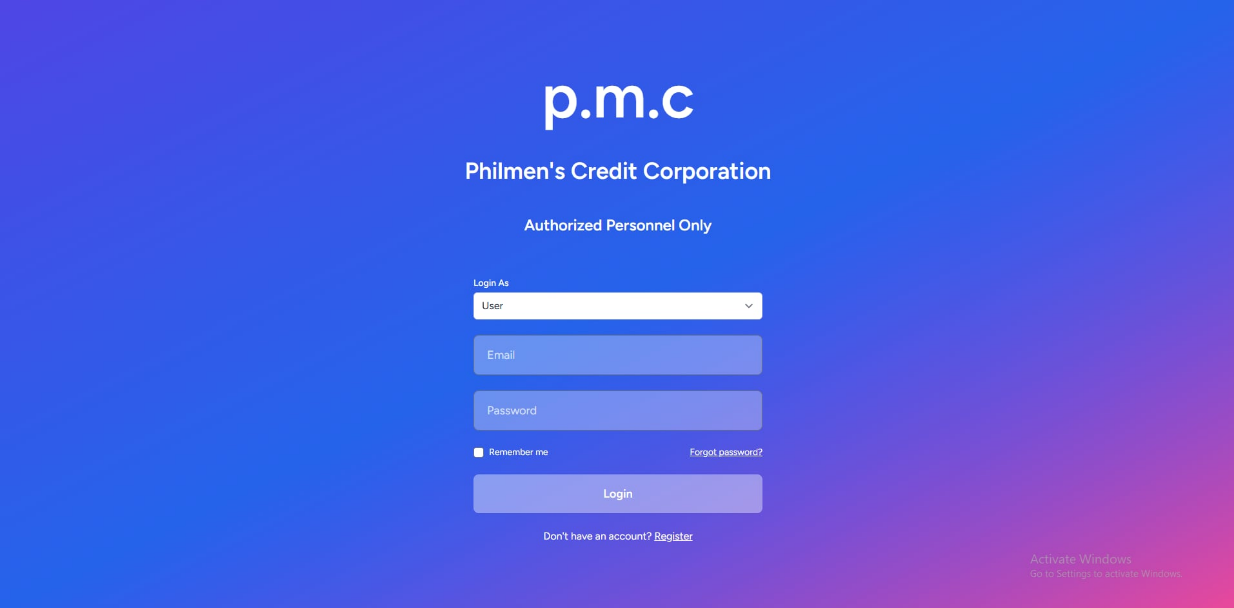
****

* **Appendix B:** Full Set of User Stories

|  |  |  |
| --- | --- | --- |
| User Story | | |
| People User Persona | I want to <Goal/Objective> | So that <benefit/result/some reason> |
| Philmen’s Credit Corporation Employee | Implement a unified system for all financial operations. | To eliminate integration issues between different platforms, ensuring data accuracy and streamlining workflows. |
|  | Develop an advanced security and threat protection system. | To protect against cyber threats and scams, securing large transaction volumes and preventing data breaches. |
|  | Create a robust and automated compliance management module. | To automatically track and update regulatory rules, reducing the risk of non-compliance and ensuring reports are generated accurately and on time. |
|  | Deploy an automated backup and recovery solution. | To continuously back up data and enable instant recovery, increasing reliability and reducing reliance on manual daily processes. |
|  | Integrate a built-in user support and training system. | To reduce user errors and improve system adoption by providing interactive guides, tooltips, and training dashboards for employees. |

* **Appendix C:** API Documentation



* **Appendix D:** Full Design Mockups

