Software Requirements Specification (SRS) Template
(Delete this page after reading/before submission)

In this template you will find text bounded by the "< >" symbols. This text appears in italics and is intended to guide you through the template and pcomprovide explanations regarding the different sections in this document. There are two types of comments in this document. These comments that are in black are intended specifically for that course. These comments that are in blue are more general and apply to any SRS. Please, make sure to delete all of the comments before submitting the document.

The explanations provided below, do not cover all of the material, but merely, the general nature of the information you would usually find in SRS documents. Most of the sections in this template are required sections, i.e. you must include them in your version of the document. Failure to do so will result in marks deductions. Optional sections will be explicitly marked as optional. >

Please write 'to the point text' in this proposal. No lengthy stories!

Maintain version history here

VERSION 1.0.0

PROJECT PROPOSAL

VERSION HISTORY				
VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
1.0.0				

Software Requirements Specification

for

Zaamin

Prepared by <group 13>

Hajra Tarar

Rabi Hussain

Maham Zahid

Maria Malik

Sherry

Date <dd-mm-yy>

Effort <# of hrs spent on this document>

Instructor Maryam Abdul Ghafoor

SBASSE-LUMS

Contents

Contents

1 Introduction

1.1 Proposal

<TO DO: Please add your entire proposal document here with approved features. If your project is different with what you have submitted then add scope, business drivers and featuresM as discussed with your TAs >

1.2 GitHub Setup

Github Repository*:* Zaamin: A secure data portal with encryption and security (github.com)

Github Board: Zaamin- A Security and Compliance Portal (github.com)

2 Overall Description

2.1 Product Perspective

Zaamin, a cutting-edge HR data management portal, emerges as a pivotal replacement and security solution for the existing systems within the Devsinc ecosystem. Positioned as a standalone application, it is designed to seamlessly integrate existing HR systems, serving as a robust addition to the company's technology infrastructure. This solution is not merely a replacement for outdated systems but an evolution that addresses critical security and compliance challenges in handling employee data within the HR domain. The portal aims to provide a secure platform for HR and non-HR personnel to manage data within Devsinc.

The system design comprises three main components: the HR Data Management Module, Security and Compliance Measures, and the User Interface. The HR Data Management Module is responsible for handling the core functionalities related to employee data, ensuring smooth organization and accessibility. The Security and Compliance Measures involve encryption, multi-factor authentication, and data backup mechanisms to fortify the system against unauthorized access and data breaches. Finally, the User Interface ensures a user-friendly experience for all employees while navigating the system.

The existing HR data management systems often face unauthorized access, data theft, and data manipulation vulnerabilities. Our product focuses on rectifying these flaws by implementing state-of-the-art security measures, including end-to-end encryption, multi-factor authentication, and data recovery protocols. This proactive approach is designed to safeguard sensitive information and aligns with global privacy standards such as GDPR, ensuring that the product adheres to the highest levels of data protection.

Zaamin is tailored to meet the specific needs and permissions of HR admins, Managers, and Employees. All of them can create their accounts to access Zaamin's personalized pages based on their roles. Devsinc employees can check their financial history and the company's offered facilities, update their personal information, file complaints, and perform other job functions. None of the employees will be able to access information related to other employees. Managers will have greater access rights with the permission to see information about all department employees. HR admin can efficiently manage all personnel's records and generate insightful reports through the intuitive User Interface. They can also track suspicious activities by analyzing audit logs and ensure regulations are followed in a compliance dashboard. The focus on user-friendly design for these interactions minimizes the need for extensive training, enhancing efficiency and engagement. This range of features offered by Zaamin streamlines data management and aligns with Devsinc's commitment to global compliance standards.

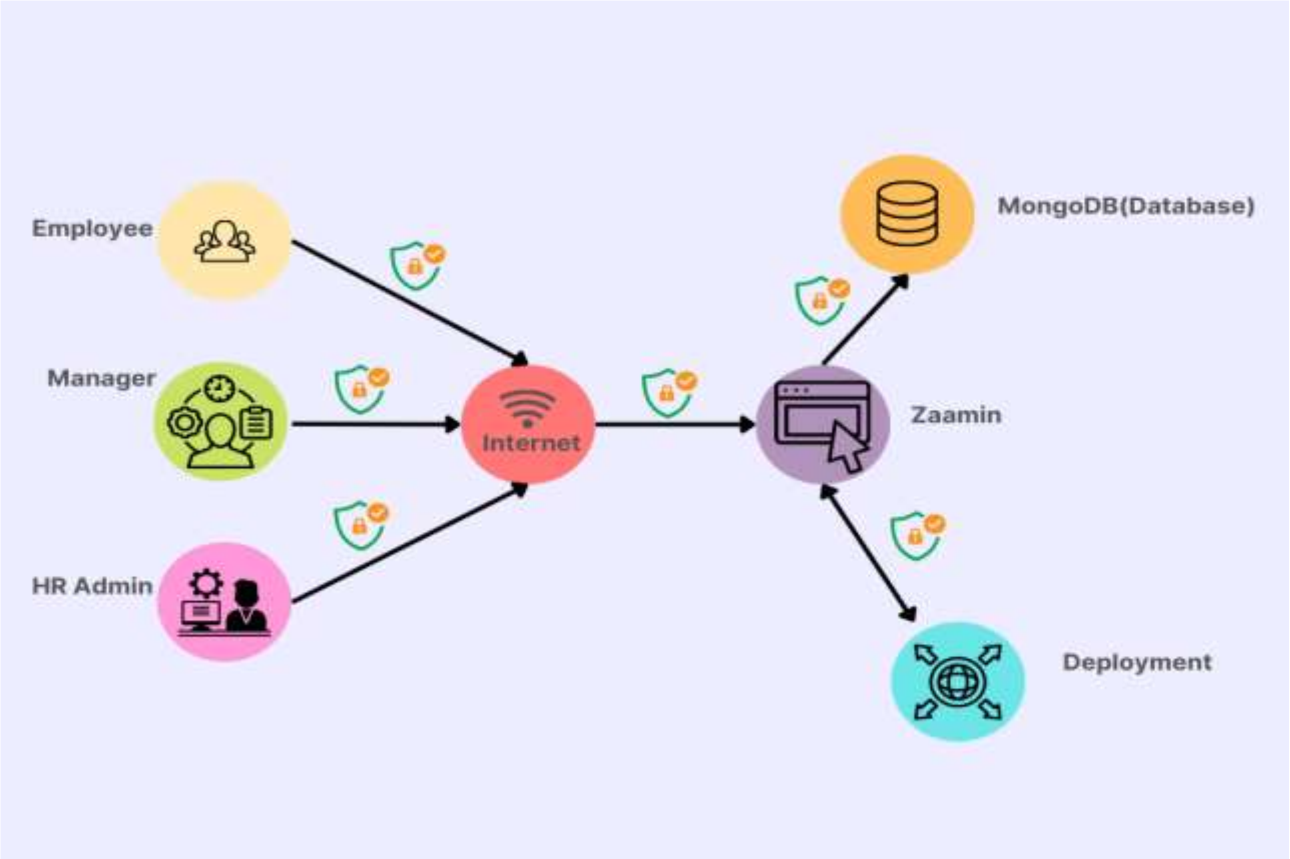


Figure 1: Flow diagram of how Zaamin will be used

2.2 Product Features

2.2.1 Account Management:

- **User Sign Up**: Admin, Managers and Employees can create an account to access the HR portal upon Employment Confirmation to protect Zaamin from outsider's attacks. Pre-existing account checks and input validation will be applied before allowing the user to successfully sign up.
- **User Login**: Admin, Managers, and Employees can access their accounts by entering correct credentials for multi-factor authentication. The users will be given fixed number of attempts to login, if failed the Account will automatically be locked and the user notified for safety purposes.
- **User Logout**: A sign-out button to allow the users to logout and be redirected back to the Login page.
- **Forget Password**: Users will be redirected to a new page to verify their identity before allowing them to change their password. Multi-factor authentication, using OTP and security questions will be deployed here.
- **Update Password**: Users will be redirected to a new page to verify their identity before allowing them to change their password. This will include confirming their own password, followed by OTP/security questions for authentication.

2.2.2 Profile Management:

- Users will be able to view and update their personal information, such as email address, phone number, home address, emergency contact information and other relevant information.
- HR administrators will be able to update employee statuses.

2.2.3 Medical Center:

- Users will be able to view and update and view their health insurance information, medical history, information regarding available healthcare providers, coverage details, and submission of medical claims.

2.2.4 Financial Center:

- Users and HR utilize this section for payment management and tax information.
- It facilitates tasks like accessing payment information, managing tax documents, and overseeing employee benefits.

2.2.5 Navigation Bar/Menu:

- This feature provides easy access to different sections and features of the HR portal through a well-organized and intuitive menu. It ensures users can quickly navigate between sections like profile management, financial center, medical center, and more.

2.2.6 Audit Log Generation:

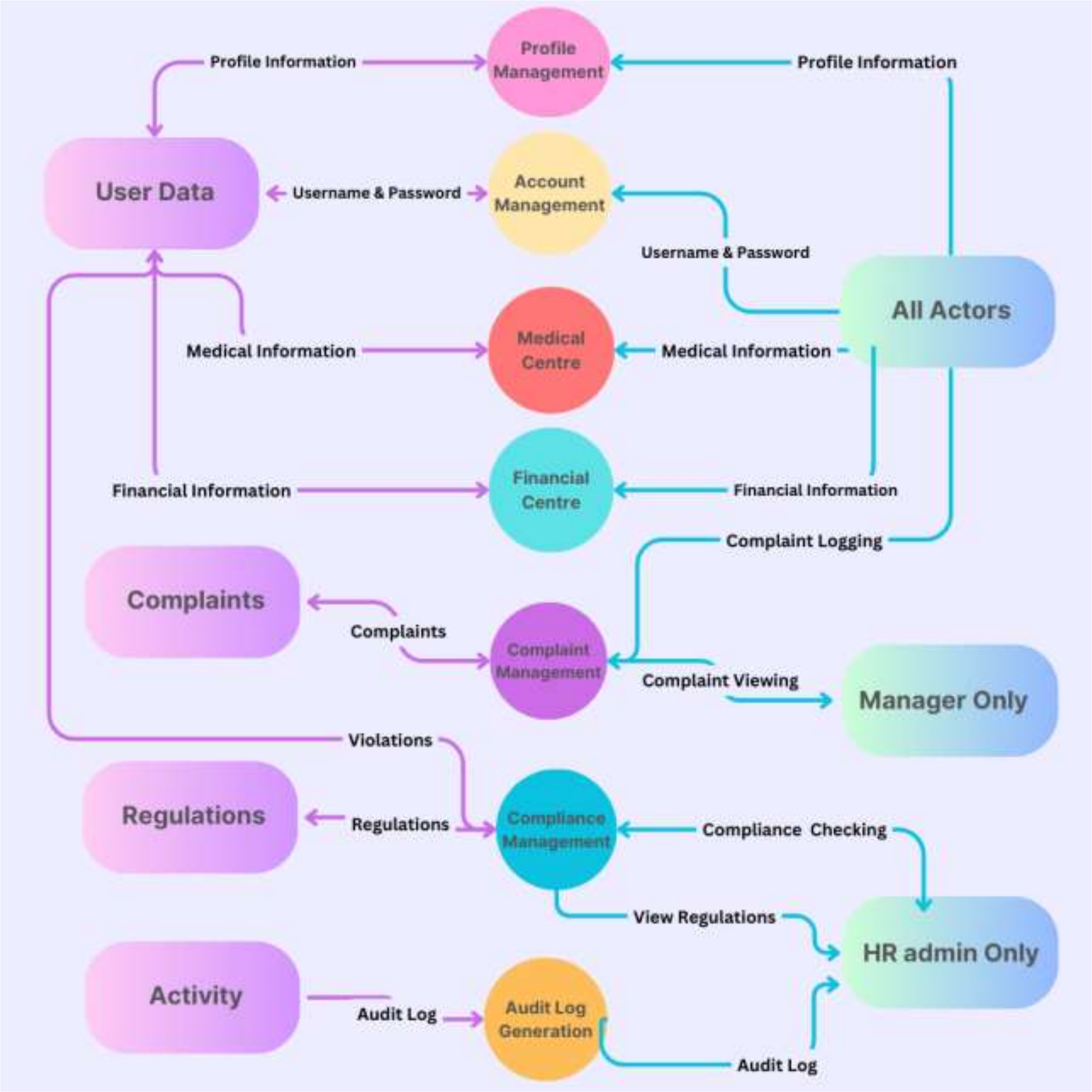
- **Generate Audit Log:** Users can create an ad hoc audit log.
- **Filter Audit Log:** Users can filter audit logs by timestamp, department, or person.
- **Export Audit Log:** Users can export the audit log as either a pdf or a csv.

2.2.7 Compliance Management

- **Overall Status:** Users can see a color-coded number representing overall compliance status.
- **View Violations:** Users can view outstanding violations based on entered regulations.
- **View Regulations:** Users can view regulations entered in the system.
- **Add Regulation:** Users can add a new regulation into the system.
- **Remove Regulation:** Users can remove an existing regulation from the system.

2.2.8 Complaint Logging/Tracking

- **Log a Complaint:** Employees can log a complaint by filling out the relevant form.
- **Complaint Status:** Employees can see logged complaints and their status.
- **View/Resolve Complaint:** HR Admins / Managers can view and resolve logged complaints.



2.3 Users and Characteristics

2.3.1 HR Admin:

Will have the most access rights.

- Can view and analyze audit logs for all departments.
- Can view and oversee filed complaints from all departments.
- Can view and edit (after consent) employee information.
- Can generate different forms.
- Can generate Insightful reports.

- Compliance Dashboard (can view violations, add regulations, remove regulations)
- Can take corrective actions and initiate compliance-related processes.
- Can create, modify, and deactivate user accounts.

2.3.2 Manager:

Will have second most access rights.

- Each manager of a department can view information about their department employees.
- Can process leave requests.
- Can view audit logs of their department.
- Can view filed complaints.
- Can access employee training and development records for their department.

2.3.3 Employees:

Will have the least access rights.

- Can access financial-related features such as salary details, tax information, etc.
- Can submit leave/absence requests.
- Check the status of requests.
- Can view and edit their own personal information only.
- Can log complaints they encounter within the organization.

2.4 Assumptions

2.4.1. Assumptions:

- All users, including the HR admin, managers, and employees, must have a stable internet connection and a web browser to utilize Zaamin.
- User's network infrastructure is equipped with firewalls and intrusion detectors to mitigate vulnerabilities and prevent unauthorized access.
- Users need to be familiar with navigating English-language websites.
- Users, including HR admins, are presumed to possess adequate training in best practices for security and compliance requirements, minimizing potential vulnerabilities stemming from user actions.
- Data collection, storage, processing, and sharing of data adhere to both National and International legal frameworks.
- It is assumed that the data inputted by HR admin, managers, and employees is accurate and up to date. Any miscommunication resulting from inaccuracies in the entered data falls outside the scope of our responsibility.
- Any employee can sign up to access the HR Portal upon verification of their employment status. Therefore, no limit on the number of users that can be signed up (but presumed to be not more significant than the total number of employees at Devsinc).
- The number of managers is assumed to be fewer than employees.

2.4.2. Constraints:

- The integration of the HR portal with existing systems imposes limitations on the introduction of new security protocols, thereby restricting the extent to which security measures can be implemented.
- The project is subject to compliance requirements that may undergo changes over time, and its development is bound by the necessity to adapt to any new regulations introduced after the initial development phase.
- The security features of the HR portal may experience constraints based on the compatibility of various security measures with different devices and browsers.
- It is crucial to ensure that the implementation of security measures does not compromise the user-friendliness and overall acceptance of the portal by end-users, as an excessive focus on security may negatively impact user experience.

2.5 Operating Environment

Zaamin is expected to smoothly operate on popular browsers like Google Chrome, Microsoft Edge, and Mozilla Firefox, as well as across various operating systems, including Linux, Windows, Ubuntu, and MacOS. While it ensures seamless functionality across diverse environments, its peak performance is anticipated on Windows, emphasizing user-friendly adaptability.

3 Specific Requirements

3.1 Functional Requirements

<Category: Sign Up>

RQ <1> Manager Sign Up	
Description	The system allows a manager to sign up using their credentials
Input	Fields: Name, username, ID, email, password + Sign Up button
Processing	The user’s ID will be used to verify their manager status. Their username will be compared to existing usernames to make sure it’s unique. All inputs (such as email) will be validated. The password will be entered twice for confirmation and captcha for human confirmation.
Output	Upon successful sign up, the user will see a success message and be redirected to the dashboard/site entry point. Upon failure, the user will see an error message displayed on the screen and the option to try again.

RQ <2> Employee Sign Up	
Description	The system allows an employee to sign up using their credentials
Input	Fields: Name, username, ID, email, password + Sign Up button
Processing	Their username will be compared to existing usernames to make sure it's unique. The password will be entered twice for confirmation and checked for strength. All inputs (such as email) will be validated. A captcha may be required for human confirmation.
Output	Upon successful sign up, the user will see a success message and be redirected to the dashboard/site entry point. Upon failure, the user will see an error message displayed on the screen and the option to try again.

RQ <3> HR Admin Sign Up	
Description	The system allows an HR admin to sign up using their credentials
Input	Fields: Name, username, ID, email, password + Sign Up button
Processing	The user's ID will be used to verify their admin status. Their username will be compared to existing usernames to make sure it's unique. The password will be entered twice for confirmation and checked for strength. All inputs (such as email) will be validated. A captcha may be required for human confirmation.
Output	Upon successful sign up, the user will see a success message and be redirected to the dashboard/site entry point. Upon failure, the user will see an error message displayed on the screen and the option to try again.

RQ <4> Update Password	
Description	The user(s) can update their password
Input	Old password, new password, new password (again)
Processing	The new password's strength will be checked and displayed with suggestions on how to improve it. A captcha may be required for human verification.
Output	If the password is successfully changed, the user is notified accordingly. If not, the user sees an error message.

<Category: Audit Logging>

RQ <5> Generate Audit Log	
Description	The user can generate an audit log.
Input	The user can generate an audit log through a button

Processing	The system generates and displays a log of activities that recently occurred on the system: specifically, the timestamps, event, and user information.
Output	Upon success, the user sees an audit log displayed in the web page. The user can scroll up and down to view.

RQ <6> Filter Audit Log	
Description	The user can filter the audit log by department, person, date.
Input	Date Range (date picker) / Department (drop down) / Person (ID-based Search box / drop down) + Button to Filter
Processing	The system filters the results of the audit log based on the search criteria
Output	The system displays an audit log limited to the criteria. If the criteria is not matched at all, an error message is displayed.

RQ <7> Export Audit Log	
Description	The HR admin can export the audit log
Input	The user can click on a dedicated button to export the displayed log
Processing	The system creates an ad hoc report in pdf/csv format, verifies the user identity through password/MFA.
Output	If user authentication is successful then the log is downloaded successfully, otherwise an error message is displayed to the user.

<Category: Compliance Dashboard>

RQ <8> View Violations	
Description	The HR admin can view violations of the regulations
Input	The user can navigate to the compliance dashboard to see open violations in the data portal and fix them
Processing	The system displays the non-compliant data in a tabular/list form and applies any fixes that the user makes and stores the result in the database.
Output	The user sees a success/failure message

RQ <9> Compliance Status	
Description	The HR admin can see the overall compliance status
Input	The data present in the databases and regulations

Processing	The system computes the overall compliance status by seeing how many violations there are and their severity and mathematically processing it.
Output	The user can see the overall status, colored by severity (red, yellow, green).

RQ <10> View Regulations	
Description	The HR admin can view all regulations
Input	The HR admin must navigate to the page using a button on the compliance dashboard
Processing	The systems display the regulations from the database they are stored in in a tabular/list format
Output	A list of regulations

RQ <11> Add Regulations	
Description	The HR admin can add a new regulation
Input	The user must enter the parameters of the regulation using keyboard input and dropdown input methods to choose what fields the regulation applies to and what the threshold will be etc. The user must also authenticate before the regulation can be added.
Processing	The system stores the new regulation in a database
Output	The user sees a success/failure message and the regulation is added to the list in ‘View Regulations’.

RQ <12> Remove Regulations	
Description	The HR admin can remove a regulation
Input	The user must click on the button to delete the regulation. The user must also authenticate before the regulation can be removed.
Processing	The system removes the regulation from the database
Output	The user sees a success/failure message and the regulation is removed from the list in ‘View Regulations’.

<Category: Login>

RQ <13> Manager Login

Description	Managers shall obtain access to their accounts through the provision of their distinctive username and password, in addition to the input of a one-time password (OTP).
Input	Fields: username, password + OTP + Login button
Processing	The system will authenticate the manager's identity by comparing the provided password with the securely hashed password stored in the backend database. If the credentials match, the manager will be granted access to their account. Otherwise, they will be prompted to re-enter their credentials for security purposes.
Output	Access granted to Manager dashboard and administrative tool

RQ <14> HR Admin Login	
Description	HR Admin shall obtain access to their accounts through the provision of their distinctive username and password, in addition to the input of a one-time password (OTP).
Input	Fields: username, password + OTP + Login button
Processing	The system will authenticate the manager's identity by comparing the provided password with the securely hashed password stored in the backend database. If the credentials match, the manager will be granted access to their account. Otherwise, they will be prompted to re-enter their credentials for security purposes.
Output	Access granted to HR Admin dashboard and Administrative Tools (Based on their level of clearance and job)

RQ <15> Employee Login	
Description	Employee shall obtain access to their accounts through the provision of their distinctive username and password, in addition to the input of a one-time password (OTP).
Input	Fields: username, password + OTP + Login button
Processing	The system will authenticate the manager's identity by comparing the provided password with the securely hashed password stored in the backend database. If the credentials match, the manager will be granted access to their account. Otherwise, they will be prompted to re-enter their credentials for security purposes.
Output	Access granted to Employee dashboard and tools relevant for updating their own data

RQ <16> Forgot Password	
Description	The user can reset their password if they forget it.

Input	OTP, New password (twice for verification), Captcha for human verification
Processing	The user is redirected to a new page from a forgot password button where they must verify their email and identity with either a timed OTP/MFA. Upon successful verification, they can change their password, which is encrypted and stored in the system.
Output	The user is redirected to their entry point based on their role or an error message is displayed in case of failure.

<Category: Navigation Bar/Menu>

RQ <17> Navigation Bar	
Description	The navigation bar displays a list of pages or options available for users to navigate to.
Input	Press the button/tab representing the navigation bar icon on the corner of the screen and choosing the page to navigate to.
Processing	The system redirects the user to the page selected.
Output	The user is redirected to the selected page.

RQ <18> Recently Visited	
Description	This option displays a list of the pages most recently visited within the HR portal
Input	Press the button/tab representing the Recently visited icon
Processing	Up to a specific number of most recently used URLs would be stored along with timestamps. Pages would be managed using the Least Recently Used (LRU) policy, removing the oldest entries when the maximum limit is reached
Output	The system displays a list of the recently visited pages, showing their titles or URLs.

RQ <19> Profile	
Description	Allows users to view and edit their personal profile information.
Input	Press the button/tab representing the Profile icon
Processing	Securely manage and provide access to personal data.
Output	Display user's profile details and enable editing options if permitted.

RQ <20> Financial Account	
Description	Provides access to financial-related features such as salary details, tax information, etc.

Input	Press the button/tab representing the Financial Account icon
Processing	Retrieve and update financial data from the HR database or integrated financial systems.
Output	Display financial account details and other relevant financial information.

RQ <21> Leave / Absence Requests and their Status	
Description	Enables employees to request leaves or absences and check the status of their requests.
Input	Enter the relevant request; Press submit button. Press Status button to view status
Processing	Handle leave request submissions, approvals, rejections, and updates in real-time.
Output	Display a list of leave requests along with their current status (pending, approved, rejected).

RQ <22> Medical Centre	
Description	Facilitates access to medical-related features such as health insurance, medical history, etc.
Input	Press the button/tab representing the Medical Centre icon
Processing	Securely manage and provide access to medical records and related data.
Output	Display medical information and related features like insurance details, medical history, etc.

RQ <23> Logging/Filling a complaint	
Description	Allows employees to log complaints or issues they encounter within the organization.
Input	Enter the relevant request; Press submit button. Press Status button to view status of complaint.
Processing	Route complaints to relevant departments or personnel for resolution
Output	Confirmation of complaint submission and tracking mechanism to monitor complaint status.

RQ <24> Viewing Complaints	
Description	Allows admin to view complaints or issues employees encounter within the organization.
Input	Press the button/tab representing the View Complaints icon
Processing	Retrieve and display all complaints filed and change their status
Output	Admins can view all complaints filed and their current status, facilitating the management and resolution process.

RQ <25> Viewing and Editing Employee Rank	
Description	Allows admin to view employee's rank and promote and demote them as per the company's requirement
Input	Select the "View" option, and if changes are required, make adjustments to the rank, and press the submit button.
Processing	Retrieves and Displays employees' rank
Output	Admins can view all employees and their current rank facilitating the management and resolution process.

3.2 External Interface Requirements

3.2.1 User Interfaces

Zaamin will be a web-based application designed to be accessible on a wide range of operating systems, including but not limited to Windows, macOS, and Linux, and can be accessed on supported browsers within the OS, such as Chrome, Edge, Safari, Opera or Firefox. Zaamin may not support outdated or depreciated browsers, such as Internet Explorer. Users can interact with Zaamin's services using a GUI (Graphical User Interface) and standard input methods such as keyboard, mouse, or touch input. The website does not require extraneous software/hardware but does assume a stable internet connection is available to the user.

The target audience for Zaamin are office workers (managers, employees and HR admins), so we assume that they are familiar with web browsing and interacting with websites. However, we will try to make the website accessible for differently abled users to the best of our ability by providing alternate text for images and video captioning where possible, multiple means of navigation for users restricted to keyboard navigation and the use of semantic HTML and ARIA (Accessible Rich Internet Applications) roles for ease of access with screen-readers and other assistive technologies.

3.2.2 Software Interfaces

Zaamin will be a website available across all major operating systems (Windows, Mac, Linux). Because the development environment primarily relies on Windows, the website is designed to function optimally on this platform.

Zaamin will be built on the MERN stack, comprising MongoDB for database management, React for the front-end development, and Node.js for server-side operations. HTML and CSS will also be used to improve usability.

To ensure a secure and dependable browsing experience for users, Zaamin will integrate libraries such as Auth0 for streamlined authentication and authorization processes, Forge for advanced cloud-based APIs and services, and CryptoJS for implementing cryptographic functions such as encryption and hashing. This comprehensive approach aligns with the website's commitment to user privacy and data integrity.

Upon deployment, Zaamin will be hosted on a secure HTTP platform to ensure a safe and reliable browsing experience for the users.

The system might send profile data across software components when authenticating users, or updating the user’s profile (such as when the password is updated). Similarly, any external API calls may contain internal data to get personalized results, or data needed by the system for processing.

4 Non-functional Requirements

4.1 Performance Requirements

1. **User Authentication efficiency:**

Login, signup, and access verification processes within the HR portal must be completed within 8 seconds, ensuring a seamless and secure user experience. The 2-factor authentication code sent via mobile SMS/email must be designed for heightened security; it should expire after 30 seconds of non-use. To maintain security protocols, a new authentication request must be initiated after the expiration period, ensuring the timely verification of user identity for enhanced access control and protection of sensitive HR data.

2. Data Retrieval Response Time:

The retrieval of sensitive HR data of a single employee should not take more than 5 seconds. This is essential to compliance verification and ensures optimal data accessibility without compromising security.

3. Audit Log processing Time:

Processing and analysing audit logs for security and compliance processes should be completed within 15 seconds. This is crucial for identifying and responding to security incidents swiftly, ensuring compliance with regulatory standards.

4. Real time Alerts:

The delivery of real time alerts for suspicious activities or security breaches must occur within 3 seconds of detection. This will enable swift response to potential threats and will reduce the impact of the security incidents. This will also facilitate compliance with reporting requirements.

5. System Scalability:

The portal design must gracefully accommodate a concurrent employee load of at least 5,000 users without compromising performance or speed. This scalability is vital for adapting to growing employee bases and peak usage periods, guaranteeing consistent and optimal performance even during high-demand scenarios.

6. Cross-Browser Compatibility and Accessibility:

Zaamin's performance and reliability are underlined by its seamless compatibility across all major browsers, including Google Chrome and Microsoft Edge. Accessible from any desktop device, the sole requirement is a reliable internet connection. This commitment to versatility ensures users can effortlessly engage with Zaamin across different platforms, emphasizing a user-friendly and accessible experience regardless of the chosen device or browsing preference.

7. User Centric Personalisation:

Zaamin is required to provide a user-centric and personalized design, avoiding unnecessary complexity. Tailored to meet HR-specific needs, the system will feature a streamlined, intuitive, and lightweight interface. The ultimate goal is to deliver a cost-effective solution which enhances user adaptability and simplifies training efforts, showcasing a commitment to user satisfaction and personalized functionality.

8. Reliability:

Zaamin must ensure that the data is backed up to the database frequently. This is to ensure that in case of data loss, it can be recovered quickly. Frequent checking of the website for reliability issues should also be done.

4.2 Safety and Security Requirements

1. User Authentication

Zaamin must guarantee a secure login system using Multi-Factor Authentication to ensure that only personnel with the given access rights can successfully log in to the portal. Access to the website should be restricted to only the company's administrators, managers, and employees to protect the system from unauthorized access and potential third-party breaches. The Multi-Factor Authentication process should add additional layers of security, along with username and password, requiring users to verify their identity through multiple means, especially when accessing or altering sensitive information (changing password). The extra factors would belong to the following categories: something you have (OTP/tokens) or something you know (further questionnaires). A different implementation of temporary account lockouts after multiple failed login attempts and notifications regarding such suspicious activity is needed to prevent brute force attacks.

2. Input Validation

There is a need for strict user input validation mechanisms to ensure that the HR Portal is safeguarded against malicious activities like SQL injections or cross-site scripting attacks. Rigorous input validation ensures that only authorized and correctly formatted data is accepted, reducing the risk of unauthorized access or manipulation of sensitive HR data. For the authentication process, input validation is essential to enforce constraints on entering emails and passwords. The website must ensure that passwords adhere to specific strength criteria, the ISO 27001 Requirements for password security, to ensure data security and compliance with regulatory standards, contributing to the HR portal's overall trustworthiness and reliability.

3. Authorization

The HR portal must ensure that only authorized individuals with the relevant permissions are granted access to sensitive HR resources. Role-Based Access Control (RBAC) and Permission-Based Access should be implemented to assign access based on pre-defined user roles. Only admins should have access to confidential HR documents, such as employment contracts, non-disclosure agreements, and legal correspondence. Therefore, each actor must only be allowed to sign-up/log-in in their field. Overall, users like employees must only be given the minimum level of access necessary to perform their job functions to minimize the potential impacts of a security breach (Least Privilege Principle).

4. Encryption:

Encryption is necessary to ensure that data, in transit and at rest, is safe from unauthorized access and various data breaches. Transport Layer Security (TLS) for data in transit safeguards must be employed against third-party interception to offer secure communication between users and the HR server. Additionally, sensitive HR data at rest, including employee records and payroll information, must undergo encryption on servers and databases. Furthermore, Zaamin should be committed to enhancing the security of user passwords during sign-up by employing a secure hashing process, which generates an irreversible, fixed-size string of characters. This measure should be implemented to fortify security and ensure the safety of user credentials. Thus, implementation of encryption is necessary to ensure that Zaamin’s security and data protection and is dedicated to data privacy and compliance requirements.

5. Data Privacy:

The Portal must ensure compliance with GDPR standards and the Pakistan Data Protection Act of 2021, emphasizing confidentiality. This commitment must be reinforced through consent management, empowering employees to control their data collection, processing, and storage. Users have the right to modify or delete information in the database, ensuring transparency and user agency. Additionally, Zaamin’s practices must adhere to data minimization, collecting and retaining only essential HR information, further promoting confidentiality, and aligning with stringent data protection regulations. Confidentiality is to be implemented, reflecting Zaamin’s dedication to safeguarding sensitive information and preserving user privacy.

6. Audit Logging:

The website is required to document user activities within the HR system to verify whether actions align with the company’s established policies and regulations and to analyze and investigate activity in case of security breaches. Each user interaction, including data access and modifications, must be logged to ensure user accountability and non-repudiation. It is necessary that the logs should adhere to privacy policies to provide a safe environment to the users. The integrity and confidentiality of the personnel must be safeguarded and unauthorized alterations to the trails prevented with the deployment of access control lists. This comprehensive approach aligns with the security goal of accountability and is instrumental in determining the attacker or principal when facing any security incidents. To meet the specified requirements, secure timestamping should be employed for accurate event sequencing, and data integrity measures to ensure that the logs and audit trails remain unaltered, preventing any attempts to cover tracks. Collectively, these practices must be implemented to provide a secure, compliant, transparent HR portal for the end users and the company.

7. Threat Detection.

Threat Detection on account of any suspicious activity as briefly introduced earlier, such as continuous unauthorized access or modifications, is essential to protect the integrity, availability, and confidentiality of data. The system must include an automated response system to alert and trigger immediate action upon early identification of possible security threats. Specifically, an email alert should be sent to the respective employee notifying them of the suspicious activity. Concurrently, an alert must also be sent to the responsible HR administrator for further investigation. To ensure security, the employee's account needs to be automatically locked, requiring the individual to undergo a verification process using multi-factor authentication before reinstating account access.

4.3 Software Quality Attributes

4.3.1. Correctness

- Zaamin must ensure that the software operates reliably and accurately, particularly with regards to managing and updating sensitive HR data.
- The system should ensure that security controls, such as access controls, encryption algorithms are accurately implemented and function as intended.
- The product must guarantee the accurate implementation of user authentication and authorization processes, ensuring that only authorized individuals have access to sensitive resources.
- The system must align its behavior with established security policies, and regulatory requirements.
- It also necessitates the validation of security processes through rigorous testing, including manual testing, vulnerability assessments, and code reviews.
- There needs to be a data validation mechanism to ensure the accuracy and integrity of HR data.

4.3.2. Availability

- It is essential to ensure the HR portal’s availability for continuous access to sensitive HR data and providing service even during security measures or compliance checks.
- The system should employ a data backup system to ensure consistency and recoverability of data in case of a system failure.
- Implementing replication through MongoDB's replica sets is integral to the HR portal's availability strategy. Replication enhances the system's resilience, contributing to continuous availability and mitigating the impact of potential node failures.
- The system should also leverage from cloud computing and the provided cloud-specific features such as automated backups, automatic scaling, and high availability configurations for availability.
- Incorporating these measures ensures that the HR portal maintains high availability, even under challenging circumstances, and is well-prepared for unforeseen attacks.

4.3.3. Flexibility

- The HR portal should be designed as a flexible system that can easily integrate new features or modify the existing ones with evolving HR standards and users.
- It must also be able to adapt to changing compliance requirements and security protocols using agile updates and response systems.
- The system should implement features that facilitate seamless integration with evolving HR technologies. Open standards and protocols are required to allow integration with systems other than Zaamin. Protocol formats like JSON should be used to transfer code between systems quickly.
- To provide further flexibility to the users, user customization based on the roles and preferences of the users needs to be deployed.
- The website must be compatible across different operating systems - Windows, Mac, and Linux- and should function irrespective of the underlying hardware to promote a design that enhances versatility.
- All these measures for maintaining a flexible system are necessary for Zaamin to evolve with HR needs continuously, ensuring long-term adaptability and responsiveness in meeting organizational and user requirements.

4.3.4. Maintainability

- Zaamin must provide a well-documented source code so other developers can easily comprehend and maintain the system’s security features.
- Zaamin should be developed with a modular and scalable code structure to enhance the maintenance of the user interface along with the security requirements.
- The development should follow a microservice architecture to enhance user interface and security maintenance by allowing independent updates to specific microservices, like payroll tracking, without affecting the entire system.
- Regular code review processes are required to ensure the code adheres to secure coding practices, standard conventions, and design principles.
- The system should utilize version control systems, such as Git, to maintain an organized history of changes.
- Regular security audits and vulnerability assessments must be conducted on the code to ensure consistent, ongoing, and **Data Security and Compliance**.

5 Backlog Tracking

5.1 Product Backlog

Business Requirement (ID)	001

User story	As a user, I want to securely sign up so that I can properly be integrated into the company and access the information and services I need, without the risk of a security breach.
Acceptance criteria	And I know I am done when: • I input my name, username, ID, email, password in the registration page, and receive a message indicating successful signup. • My password is encrypted and saved in the database along with all my other details. • I am redirected to the home page, specific to my role (employee, manager, or HR admin). • I can view my profile after clicking on the icon in the home page.
Priority	3
Estimate	8 hours

Business Requirement (ID)	002
User story	As a user, I want to build and edit my profile on the portal, so that I can ensure my personal details on the portal are accurate and up to date.
Acceptance criteria	And I know I am done when: • I log in and click on my profile icon, I am redirected to my profile page. • I have the option to edit my profile picture, address, age, contact details and financial information (banking details). • I can select either of the options and change the information. • When clicking ‘save’, the information is saved in the database, and can be visible on my profile page.
Priority	3
Estimate	8 hours

Business Requirement (ID)	003
User story	As an HR admin, I want to be able to view and filter audit logs, so that I can detect any suspicious activity to ensure security.
Acceptance criteria	And I know I am done when: • After signing into the home page, I click on the required button to generate audit logs, I can see a log of activities that recently occurred on the system, precisely, the timestamps, event, and user information. • When choosing the option to filter by date, I can see all the audit logs of that specific date.

	• When choosing the option to filter by a certain department, I can view all the logs for that specific department. • When choosing the option to filter by ID, I can view all the logs for that specific ID.
Priority	1
Estimate	15 hours

Business Requirement (ID)	004
User story	As an HR admin, I want to be able to view or change an employee or manager's status so that the system accurately presents their current employment status and the associated access to database information
Acceptance criteria	And I know I am done when: • I click on an employee’s profile and choose the option to view their employment status. • I can view their status as well as select the edit option to change the status. • After changing the status and clicking confirm, I can see the updated change on the portal, • The employee can only access those documents that are granted to them with their updated employment status.
Priority	2
Estimate	6 hours

Business Requirement (ID)	005
User story	As a user, I want to securely login in the portal using two factor authentication so that sensitive database information is protected from unauthorized access and other potential security threats.
Acceptance criteria	And I know I am done when: • I input my login details (username and password) at the login page. • I receive a unique, system generated code sent via SMS or email and have 30 seconds to enter the code in the login page. • Upon entering the code, I am redirected to the home page associated with my specific role in the portal. • If I don’t enter the code within 30 seconds, a new code will be generated, and I have to enter that within the 30 seconds.
Priority	3
Estimate	10 hours

Business Requirement (ID)	006
User story	As a user, I want to be able to change my password so that I can maintain the security of my account and avoid unauthorized access.
Acceptance criteria	And I know I am done when: • I select on user settings option after logging into the home page and navigate to the change password option. • I input my old password and my new password (twice). • The new password's strength is checked and displayed with suggestions on how to improve it. • The system verifies if the old password is correct, and the new password meets the criteria (is of a specific length and contains a mix of special character, numbers, lowercase, and uppercase letters. • If the password meets the criteria, it is updated, and the user is notified via a popup that indicates so, as well as an email. Otherwise, the user is prompted to enter a different password.
Priority	2
Estimate	7 hours

Business Requirement (ID)	007
User story	As a HR admin, I can view violations and the overall compliance status of the company so that I can address and improve the overall regulatory status of the company.
Acceptance criteria	And I know I am done when: • I log in and navigate to the compliance dashboard, I can see an overall compliance status indicted by a percentage and colour to represent severity (red, yellow, green) • I can select the option to view violations in the compliance dashboard, where the violations are shown in a tabular format. • I can select the option to potentially fix a specific violation, upon which I receive a message indicating success or failure.
Priority	1
Estimate	15 hours

Business Requirement (ID)	008
User story	As a HR admin, I can view, add, or remove regulations so that I can maintain the compliance framework of the company.

Acceptance criteria	And I know I am done when: • After navigating to the compliance dashboard, I can select the option to view regulation, and am given a list of all regulations being followed. • After selecting the option to add a regulation, I am prompted to enter the parameters of the regulation using keyboard input and dropdown input methods to choose what fields the regulation applies to and what the threshold will be. • When selecting the option to remove a regulation, I must select the specific regulation, and be prompted to authenticate before the system proceeds to remove the regulation. • I should receive a message indicating success or failure when adding or removing a regulation and should be able to view the updated regulation list in 'View Regulation'.
Priority	4
Estimate	10 hours

Business Requirement (ID)	009
User story	As a user, I should have easy access to medical related information such as my health insurance, so that I can securely and conveniently manage my medical information.
Acceptance criteria	And I know I am done when: • I press the medical center icon and am redirected to the associated page. • I can view my personal medical information and have the option to update it. • I can view my health insurance details. • I can view my medical history when selecting the option.
Priority	2
Estimate	10 hours

Business Requirement (ID)	010
User story	As an HR admin, I want to receive real-time alerts for any security breaches, so that I can effectively respond and minimize the impacts of any potential threats.
Acceptance criteria	And I know I am done when:

	- I can receive real time alerts within one second of security threat detection. - I have the option to receive alerts via email, SMS or within the HR portal. - The alerts include more specific details such as time of the threat and the part of the system impacted.
Priority	4
Estimate	10 hours

Business Requirement (ID)	011
User story	As an HR admin, I want all data stored in the HR database to be encrypted so that sensitive information remains protected if unauthorized access to data takes place.
Acceptance criteria	And I know I am done when: - The system implements an extensive encryption process on all the data across the portal. - The data remains encrypted and safe from any breaches in transit. - The system implements a hashing algorithm to store passwords.
Priority	1
Estimate	10 hours

5.2 Sprint Number 1 Backlog

Priority	User Story	Tasks	Assigned to	Estimated time (hours)
1	As a user, I want to securely sign up so that I can properly be integrated into the company and access the information and services I need, without the risk of a security breach.	Make a signup page that takes in all the relevant user details and saves them in the database.	Hajra Tarar	3
		Input validation for all user inputs in the signup page.	Maham Zahid	2

		Password encryption and saving.	Maham Zahid	1
		Home pages for the three different roles (employee, manager, HR admin) to redirect to after signup/login.	Maria Malik	3
2	As a user, I want to build and edit my profile on the portal, so that I can ensure my personal details on the portal are accurate and up to date.	Display personal profile with all the relevant details. Set default details if any information is not given (e.g. default profile picture).	Shaharyar Ahsan	4
		Options to change the profile details and a save button to save everything in the database.	Rabi Hussain	4

Appendix B – Contribution Statement

Name	*Contributions in this phase*	*Approx. Number of hours*	*Remarks*
Maria Malik	*Section 1: Introduction* *Section 5: Backlog Tracking*	*10*	
Maham Zahid	*Section 3.1: Functional* *Section 3.2.1:Software* *Section 2.2:*		
Rabi Hussain	*Section 4: Non-functional* *Section 2: Overall Description*	*15*	*Mei toh thak gayi bhai saab*
Hajra Tarar	*Section 4: Non-functional* *Section 2: Overall Description*	*15*	*(2)*
Shahryar Ahsan	*Section 3.1: Functional* *Section 3.2.1:Users*	*15*	

Marking Rubric

Total marks: 50

Component	Marks
Github Board and Repositories	3
Product Perspective	4
Product Features	3+3 (in scope + out of scope)
Users and Characters	3
Assumptions & Operating Environment	3
Functional Requirements	10
External Interface Requirements (Users +Software)	3
Non-Functional Requirements	4
Product Backlog	4
Sprint Backlog	4
Concise and to-the-point descriptions	3
Writing Quality (Descriptions should be coherent and should covers all questions asked under the heading/follows format of document)	3