**Hamdard University**

**Department of Computing**

**Final Year Project**



**Behaviorance-I Redefining Cyber Security with Secure Sense Behavioral Compliance   
(Web Application Platform)**

**FYP-006/FL24**

**Software Requirements Specifications**

**Submitted by**

**Farwah Butt (1101-2021)**

**Emaan Nadeem (2438-2021)**

**Hafsa Khalid (2625-2021)**

**Supervisor**

**Sir Iqbal Uddin khan**

**Fall 2024**

**Document Sign off Sheet**

### **Document Information**

| **Project Title** | Behaviorance-I Redefining Cyber Security with Secure Sense Behavioral Compliance (Web Application Platform) |
| --- | --- |
| **Project Code** | FYP-006/FL24 |
| **Document Name** | Software Requirements Specifications |
| **Document Version** | 1.0 |
| **Document Identifier** | FYP-006/FL24 - SRS |
| **Document Status** | Draft/ Final / etc. |
| **Author(s)** | Farwah Butt / Emaan Nadeem / Hafsa Khalid |
| **Approver(s)** | Sir Iqbal uddin khan |
| **Issue Date** | 17-1-2025 |

| **Name** | **Role** | **Signature** | **Date** |
| --- | --- | --- | --- |
| Farwah Butt | Team Lead | C:\Users\USer\Downloads\WhatsApp Image 2025-01-17 at 2.14.35 PM.png | 17-1-2025 |
| Emaan Nadeem | Team Member 2 | C:\Users\pc.DESKTOP-B9I3J34\Downloads\WhatsApp Image 2025-01-17 at 2.39.18 PM.jpeg | 17-1-2025 |
| Hafsa Khalid | Team Member 3 | C:\Users\pc.DESKTOP-B9I3J34\Downloads\WhatsApp_Image_2025-01-17_at_3.02.06_PM-removebg-preview.png | 17-1-2025 |
| Sir Iqbal Uddin khan | Supervisor |  | 17-1-2025 |
| Mr. Suleman Ahmed Naz | Project Coordinator |  | 17-1-2025 |

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 17-1-2025 | 1.0 | Initial Version | Farwah Butt  Emaan Nadeem  Hafsa Khalid |

**Definition of Terms, Acronyms, and Abbreviations**

| **Term** | **Description** |
| --- | --- |
| Cybersecurity | Measures and practices designed to protect networks, devices, programs, and data from attacks, damage, or unauthorized access. **Reason:** Cyber Security is the core of our project. This term is critical because the entire project revolves around improving the security posture of an organization by integrating human behavioral analysis into traditional security measures. |
| Behavioral Compliance | The adherence to security protocols and policies by individuals based on their actions and behavior patterns, rather than just the implementation of technical measures. **Reason:** Our project focuses not only on technical security but also on human behavior. This term explains the human aspect of security and emphasizes that compliance is driven by behavior, not just rules. |
| Insider Threats | Security risks that come from individuals within an organization who may misuse their access to harm the organization's data or systems. **Reason:** Since our project aims to address human behavior as a vulnerability in cybersecurity, defining "insider threats" is essential to explain the specific risks posed by employees or trusted individuals. |
| Web Application Platform | A software application that is accessed and used through a web browser, often designed to perform a specific set of functions. **Reason:** Our project is building a web-based platform, and defining this term helps clarify the type of technology our using to deliver our solution. |
| IDE Tool | Integrated Development Environment (IDE), a software application used by developers to write, test, and debug code (e.g., Visual Studio Code). **Reason:** IDEs are essential for software development. Defining them helps to understand the tools our development team uses to create the platform efficiently. |
| Next Js | **Next.js** is a JavaScript framework used for the development of user interfaces, mainly SPA. Its base is React.js, and the feature added with it is server-side rendering, static site generation, and routing support.  **Reason:** React.js is the foundational technology for front-end development. Definition of Next.js clarifies how user interface is developed- mainly on factors that improve its performance and SEO ability-and highlights this within the total architecture of the project. |

# **Table of Contents**

[**Document Information** 2](#_heading=h.wtlmdtrfsfs7)

[**Table of Contents** 5](#_heading=h.dvd57yb4p6ic)

[**1.**](#_heading=h.56qlva19ez3) **Introduction** 7

[**1.1**](#_heading=h.1d79ketvleew) **Purpose of Document** 7

[**1.2**](#_heading=h.gn5jrtev6l1g) **Intended Audience** 7

[**2.**](#_heading=h.ve8cmw4ps7en) **Overall System Description** 9

[**2.1**](#_heading=h.i8wgprla0rla) **Project Background** 9

[**2.2**](#_heading=h.kq625njb64bd) **Problem Statement:** 9

[**2.3**](#_heading=h.sb63agceit07) **Not In Scope** 9

[**2.4**](#_heading=h.9swjunnqyfwh) **Project Objectives** 9

[**2.5**](#_heading=h.u8ozw98tlz47) **Stakeholders &** **Affected Groups** 10

[**2.6**](#_heading=h.j9jyws8215pe) **Operating Environment** 10

[**2.7**](#_heading=h.negh6tplv365) **System Constraints** 10

[**2.8**](#_heading=h.ynhmrc1h39o0) **Assumptions & Dependencies** 10

[**3.**](#_heading=h.6scs01wvxmo7) External Interface Requirements 11

[**3.1**](#_heading=h.dc9la6x0v6ab) **Hardware Requirement** 11

[**3.2**](#_heading=h.t8zexcgtocka) **Software Interfaces** 11

[**3.3**](#_heading=h.sdacn4lld6bk) **Communications Interfaces** 11

[**4.**](#_heading=h.vicvpmxt69u8) System Functions / Functional Requirements 12

[**4.1**](#_heading=h.xrgd4jl2fmn4) **System Functions** 12

[**4.2**](#_heading=h.bf3ny43ym5gw) **Use Cases** 13

[**4.2.1**](#_heading=h.tpasushitayr) **List of Actors** 13

[**4.2.2**](#_heading=h.ejemfpcx2dkf) **List of Use Cases** 13

[1. Sign Up Use Cases 13](#_heading=h.2unok4rgypdn)

[2. Login Use Cases 14](#_heading=h.6tq0v1p025m0)

[3. Post-Login Use Cases 14](#_heading=h.krdqpvktnpru)

[4. Navbar Use Cases 15](#_heading=h.b5827ewkb3lj)

[5. Template/Project Use Cases 16](#_heading=h.h83owqle4og3)

[**4.2.3**](#_heading=h.pmel8zgi6g8p) **Use Case Diagram** 17

[**4.2.4**](#_heading=h.odprc51vnerv) **Description of Use Cases** 17

[**Alternative Courses** 21](#_heading=h.upee7r78qtpe)

[**5.**](#_heading=h.lnzupc4mwgd7) Non - Functional Requirements 23

[**5.1**](#_heading=h.rjmek1c6ns68) Performance Requirements 23

[**5.2**](#_heading=h.60ot3c47xxt9) **Safety Requirements** 23

[**5.3**](#_heading=h.oinyzjd1n5eb) **Security Requirements** 23

[**5.4**](#_heading=h.ej5z4aknqhdp) **Reliability Requirements** 23

[**5.5**](#_heading=h.nw4j1c8yzh77) **Usability Requirements** 24

[**5.6**](#_heading=h.o84a9mqncll7) **Supportability Requirements** 24

[**5.7**](#_heading=h.1joe1uxeawpr) **User Documentation** 24

[**6.**](#_heading=h.powfpqfmacel) References 26

# **Introduction**

## **Purpose of Document**

The purpose of document section in an introduction of an SRS document states the major objectives and goals in preparing such a document. It usually includes:

* **Objective:** The project objective is to develop the smart human behavioral analysis based web application platform “Behaviorance-I”, with the predictive assessment to forecast human behavior and potential vulnerable actions
* **Scope:** The scope of project is limited to development of the Behaviorance-I web application platform with advanced integrated predictive cybersecurity and psychological assessment, build a comprehensive questionnaire bank, integration of cybersecurity and psychology principles into a unified framework..

## **Intended Audience**

The Intended Audience section defines who will read and use the SRS document. It usually contains:

* **Stakeholders:** It lists all the parties involved in the project, including developers, designers, testers, and project managers.
* **Roles:** This describes the specific role or responsibility of each stakeholder in relation to the "Behaviorance-I" web application. For instance, developers will use it to understand what features to build while testers will use it to validate the web application against requirements.

**1.3 Abbreviations:**

Abbreviations are defined in the " Behaviorance-I " SRS document to enhance clarity and uniformity in communications. They have been used throughout the document as a short hand version of frequently occurring terms phrases. Some of the examples along with their meanings are as follows:

**SRS** - Software Requirements Specification  
Refers to the document that defines all the requirements for the software.

**UI/UX:** User Interface/User Experience - The combined design and interaction considerations that aim to provide a seamless and enjoyable experience for users.

**UI** - User Interface  
Refers to the design and interaction elements between the user and the application.

**UX** - User Experience  
Describes the overall experience of a user when interacting with your platform.

**HTTPS** - Hypertext Transfer Protocol Secure  
Security protocol for safe communication over the internet, important for your platform's cybersecurity.

# **Overall System Description**

## **Project Background**

The Project Background section gives relevant background information regarding the Behaviorance-I web application platform project.  
Traditional measures of cyber security often miss the non-compliance of employees with protocols, thus leaving an organization vulnerable to risks. The Behaviorance-I platform overcomes this gap by combining human behavioral analysis with predictive cyber security to forecast and prevent actual risks that can further enhance security compliance in an organization.

## **Problem Statement:**

The Problem Statement section articulates the specific issues or challenges that the " **Behaviorance-I** web application seeks to solve. It includes

**Current Issues:**

* **Human Errors**: A large percentage of security breaches are caused by human mistakes, making them a weak link in cybersecurity.
* **Lack of Integration:** Existing cybersecurity measures do not effectively address the human behavioral aspect.

**Project Scope**

The Project Scope section defines the boundaries of the **Behaviorance-I** web application platform project.

The scope of project is limited to development of the **Behaviorance-I** web application platform with advanced integrated predictive cybersecurity and psychological assessment, build a comprehensive questionnaire bank, integration of cybersecurity and psychology principles into a unified framework

## **Not In Scope**

The Not In Scope section identifies what is explicitly excluded from the current project. It helps manage expectations and prevent scope creep by.

The platform will not track employees in real-time nor will it include training programs for the employees. Neither will the system be a part of full-fledged cyber security infrastructure to alert it regarding hackers, viruses, and more. The whole intervention into the human behavior pattern will be instant; otherwise, it'll just predict risk occurrences to nullify them afterwards.

## **Project Objectives**

The Project Objectives section outlines the goals and targets for the **Behaviorance-I** web application platform project.

The project objective is to develop the smart human behavioral analysis based web application platform “Behaviorance-I”, with the predictive assessment to forecast human behavior and potential vulnerable actions.

## **Stakeholders &** **Affected Groups**

The Stakeholders & Affected Groups section identifies all parties involved or impacted by the Behaviorance-I web application platform project.

* **Stakeholders:**  
  The key stakeholders include end users (employees), developers/technical team, and business owners. The end users will provide the data, developers will build and maintain the platform, and business owners will fund the project and enjoy improved security.

## **Operating Environment**

The Operating Environment section describes the technical and operational environment in which the **Behaviorance-I** web application platform project will operate.

* **Platforms:** Specifies the supported operating systems and devices (smartphones, tablets) that the application will run on.

## **System Constraints**

This section describes system constraints. It includes all limitations or restrictions that might impact the design or implementation of the Behaviorance-I web application platform project.

**Technical Constraints:** Behaviorance-I may have compatibility issues with older browsers or systems, limiting functionality on outdated devices or software versions.

**Non-Technical Constraints:** The project will be faced with budget, time, and resource constraints that may affect the delivery timeline and scope, thus requiring adequate infrastructure for performance.

## **Assumptions & Dependencies**

The Assumptions & Dependencies section documents the assumptions made and the external dependencies required for the Behaviorance-I web application platform project.

* **Assumptions:** User will appropriately appraise their behavior, and predictive technology works. If either assumption is violated, the performance of the platform might be adversely affected.
* **Dependencies:** Its success depends upon external factors, such as the internet and the database systems. If any of these fail, it could bring down the platform.
* **Risk Mitigation**: To manage the risks associated with assumptions and dependencies, we will use regular updates, testing, and contingency plans to ensure the project is successfully completed.

# External Interface Requirements

## **Hardware Requirement**

The system will run on standard computing devices, including desktops, laptops, and servers. It requires a minimum configuration of:

* Processor: Intel Core i5 or equivalent.
* RAM: 8 GB or higher.
* Storage: 20 GB of available disk space.

## **Software Interfaces**

The Software Interfaces section details the software systems and applications that the **Behaviorance-I** web application platform project will interact with. It includes:

* **Application**: Web Browser (e.g., Google Chrome)
* **Interface Details**: Supports browser-based interaction using standard web protocols (HTTP/HTTPS).

## **Communications Interfaces**

The Communications Interfaces section defines the protocols and communication channels that the **Behaviorance-I** web application platform project will use to interact with external systems and services. It includes

* **APIs**: May connect with third-party APIs for advanced predictive analytics or behavioral insights.

# System Functions / Functional Requirements

## **System Functions**

System functions describe what **Behaviorance-I** web application platform project is supposed to do. They are identified through the requirement gathering process with the user and may already be listed in a separate document. Here’s how to list them:

| | **Ref #** | | --- | | **Functions** | **Category** | **Attribute** | **Details & Boundary Constraints** |
| --- | --- | --- | --- | --- | --- |
| R1.1 | Predict user behavior based on inputs | EVIDENT | Response Time | Predictions should be shown within 5 seconds |
| R1.2 | Securely store user behavioral data and feedback | HIDDEN | Data Security | User data should be stored securely |
| R1.3 | Provide users with behavioral insights and recommendations | EVIDENT | Insight Generation | Insights should be provided within 5 seconds after processing user data. |

**System Attributes/ Nonfunctional Requirements**

System attributes are non-functional qualities of the system, such as performance, usability, and security. They are critical for the overall effectiveness and user satisfaction with the web application. Here’s how to define them:

| **Attribute** | **Details and Boundary Constraints** | **Category** |
| --- | --- | --- |
| Response Time | Predictions based on user behavior will appear within 5 seconds. | |  | | --- |   optional |
| Data Security | User data should be stored securely | Mandatory |
| Interface Metaphor | The system interface will be browser-based. | Mandatory |
| Concurrent User Load | A minimum of 10 users should be able to use the system simultaneously without performance degradation. | Mandatory |
| Scalability | The system should be capable of scaling up to 100 simultaneous users. | Mandatory |

## **Use Cases**

### **List of Actors**

The List of Actors section identifies the different roles or entities that interact with the Behaviorance-I web application platform. Actors are usually categorized based on their roles and responsibilities in using or operating the system. Examples of actors for your application might include:

**Users (End Users):** Those accessing the site to comply with cyber guidelines and obtain security-related recommendations.

**Admins:** Manage user data, monitor the functionality of the platform, and enforce compliance.

### **List of Use Cases**

This list of use cases will include detailed actions or activities that the user, known as the actor, carries out through the Behaviorance-I web application platform. Use cases refer to individual interactions by an actor and the system that leads to an intended outcome. Examples of the use cases of Behaviorance-I web application platform might include:

### 1. Sign Up Use Cases

**UC1.1: User Registration**

**Description**: The user clicks on the "Sign Up" button in the navbar and enters credentials (name, email, password).

**Actors**: User

**Preconditions**: User is not registered yet.

**Postconditions**: User account is created, and a verification email is sent.

**UC1.2: Email Verification**

**Description**: User enters the verification code received via email.

**Actors**: User

**Preconditions**: User has completed the registration process.

**Postconditions**: User account is verified and activated.

**UC1.3: Google Sign-Up**

**Description**: User clicks on the Google Sign-Up option and logs in using their Google account.

**Actors**: User

**Preconditions**: User has a Google account.

**Postconditions**: User account is created using Google credentials.

### 2. Login Use Cases

**UC2.1: User Login**

**Description**: The user clicks the "Login" button, enters their credentials, and logs in.

**Actors**: User

**Preconditions**: User account is already created.

**Postconditions**: User is logged in and directed to the homepage.

### 3. Post-Login Use Cases

**UC3.1: Display Welcome Screen**

**Description**: After logging in, the user sees a welcome screen with options to access a awareness or survey.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: Welcome message and buttons are displayed.

**UC3.2: Access Survey**

**Description**: User clicks on the "survey" button and is directed to a page with various question templates.

**Actors**: User

**Preconditions**: User is logged in and on the welcome screen.

**Postconditions**: User sees question templates categorized by different topics.

**UC3.3: Access** Awareness

**Description**: User clicks on the "Awareness" button and is directed to a page with information about cyber attacks.

**Actors**: User

**Preconditions**: User is logged in and on the welcome screen.

**Postconditions**: User views information about cyber threats.

### 4. Navbar Use Cases

**UC4.1: View User Profile Dropdown**

**Description**: User clicks on the profile icon in the navbar and sees options like account settings, upgrade plan, and logout.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: Dropdown menu with options is displayed.

**UC4.2: Account Settings**

**Description**: User selects "Account Settings" to reset password or change email.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: User is directed to the settings page to update information.

**UC4.3: Upgrade Plan**

**Description**: User clicks on "Upgrade Plan" to purchase or change the service plan.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: User is directed to the plan upgrade page.

**UC4.4: Logout**

**Description**: User clicks "Logout" to exit the platform.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: User is logged out and redirected to the homepage.

### 5. Template/Project Use Cases

**UC5.1: View and Edit Questionnaire Template**

**Description**: User selects a questionnaire template, answers the questions, and receives a result with security analysis.

**Actors**: User

**Preconditions**: User is logged in and has accessed the questionnaire page.

**Postconditions**: User receives a security risk analysis and suggestions.

**UC5.2: Create a New Project**

**Description**: User clicks on "Create Project" to start a new project.

**Actors**: User

**Preconditions**: User is logged in and on the dashboard.

**Postconditions**: New project is created and available for the user to manage.

**UC5.3: View or Share Template**

**Description**: User views their saved or starred template and shares it with others.

**Actors**: User

**Preconditions**: User has selected or created a template.

**Postconditions**: User can share or collaborate on the template.

**UC5.4: Save and Star Templates**

**Description**: User selects and stars a template to easily access later.

**Actors**: User

**Preconditions**: User is logged in and on the dashboard.

**Postconditions**: Template is saved or starred for easy access.

6. Dashboard Use Cases

**UC6.1: View Dashboard**

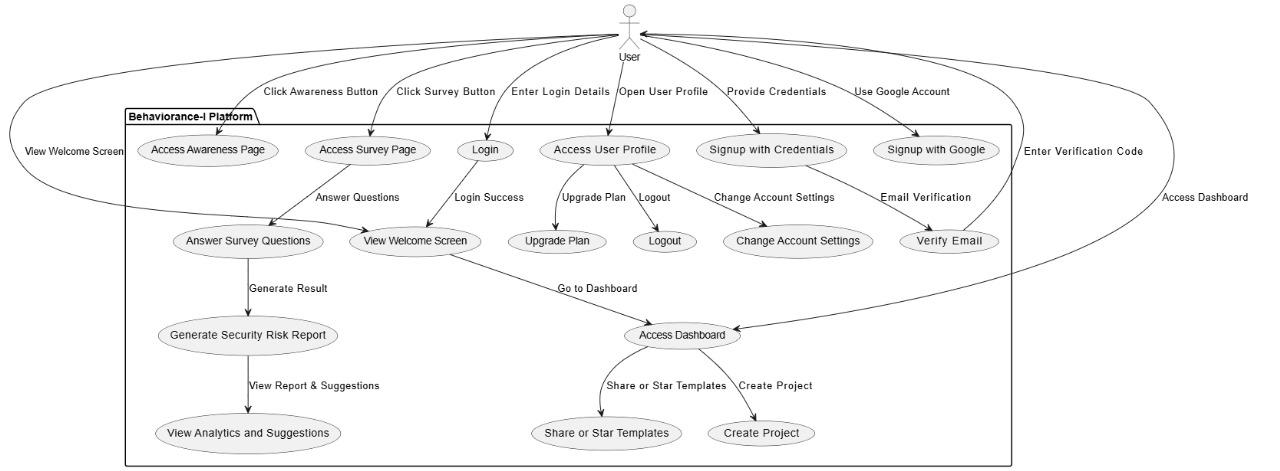
**Description**: User clicks on the "Behaviorance-I" logo to navigate to their dashboard.

**Actors**: User

**Preconditions**: User is logged in.

**Postconditions**: User is redirected to the dashboard where they can see their selected templates, projects, and actions.

### **Use Case Diagram**

**

### **Description of Use Cases**

| **Use Case ID** | **Use Case Name** | **Description** | **Actors** | **Preconditions** | **Postconditions** |
| --- | --- | --- | --- | --- | --- |
| UC1.1 | User Registration | User clicks the "Sign Up" button and enters credentials (name, email, password). | User | User is not registered yet. | User account is created, and a verification email is sent. |
| UC1.2 | Email Verification | User enters the verification code received via email. | User | User has completed registration process. | User account is verified and activated. |
| UC1.3 | Google Sign-Up | User clicks the Google Sign-Up option and logs in using their Google account. | User | User has a Google account. | User account is created using Google credentials. |
| UC2.1 | User Login | User clicks the "Login" button, enters their credentials, and logs in. | User | User account is already created. | User is logged in and directed to the homepage. |
| UC3.1 | Display Welcome Screen | After logging in, the user sees a welcome screen with options to access a questionnaire or survey. | User | User is logged in. | Welcome message and buttons (Questionnaire, Survey) are displayed. |
| UC3.2 | Access Survey | User clicks on the survey button and is directed to a page with various question templates categorized by different topics. | User | User is logged in and on the welcome screen. | User sees question templates categorized by different topics. |
| UC3.3 | Access Awareness | User clicks on the Awareness button and is directed to a page with information about cyber threats and attacks. | User | User is logged in and on the welcome screen. | User views information about cyber threats. |
| UC4.1 | View User Profile Dropdown | User clicks on the profile icon in the navbar and sees options like account settings, upgrade plan, and logout. | User | User is logged in. | Dropdown menu with options (Account Settings, Upgrade Plan, Logout) is displayed. |
| UC4.2 | Account Settings | User selects "Account Settings" to reset password or change email. | User | User is logged in. | User is directed to the settings page to update information. |
| UC4.3 | Upgrade Plan | User clicks on "Upgrade Plan" to purchase or change the service plan. | User | User is logged in. | User is directed to the plan upgrade page. |
| UC4.4 | Logout | User clicks "Logout" to exit the platform. | User | User is logged in. | User is logged out and redirected to the homepage. |
| UC5.1 | View and Edit Questionnaire Template | User selects a questionnaire template, answers the questions, and receives a result with security analysis. | User | User is logged in and has accessed the questionnaire page. | User receives a security risk analysis and suggestions. |
| UC5.2 | Create a New Project | User clicks on "Create Project" to start a new project. | User | User is logged in and on the dashboard. | A new project is created and available for the user to manage. |
| UC5.3 | View or Share Template | User views their saved or starred template and shares it with others. | User | User has selected or created a template. | User can share or collaborate on the template. |
| UC5.4 | Save and Star Templates | User selects and stars a template to easily access later. | User | User is logged in and on the dashboard. | Template is saved or starred for easy access. |
| UC6.1 | View Dashboard | User clicks on the "Behaviorance-I" logo to navigate to their dashboard. | User | User is logged in. | User is redirected to the dashboard where they can see their selected templates, projects, and actions. |
| - | Behavior Assessment | The admin feeds user behavior data into the system, and the system assesses potential security risks using predictive algorithms. | Admin, User, System | System is active, and the user is authenticated. | Admin receives a report with predictive behavioral analysis pointing out vulnerabilities. |

| **Use Case ID** | **Use Case Name** | **Actor Action** | **System Response** |
| --- | --- | --- | --- |
| **UC1.1** | User Registration | User clicks on the "Sign Up" button and enters credentials (name, email, password). | System creates a new user account and sends a verification email. |
| **UC1.2** | Email Verification | User enters the verification code received via email. | System verifies the code and activates the user account. |
| **UC1.3** | Google Sign-Up | User clicks on the Google Sign-Up option and logs in using their Google account. | System creates a new user account using Google credentials. |
| **UC2.1** | User Login | User clicks the "Login" button, enters credentials, and logs in. | System authenticates the user and redirects them to the homepage. |
| **UC3.1** | Display Welcome Screen | After logging in, the user sees a welcome screen with options to access a questionnaire or survey. | System displays the welcome message with buttons for "Questionnaire" and "Survey." |
| **UC3.2** | Access Survey | User clicks on the survey button and is directed to a page with various question templates. | System displays the questionnaire page with categorized question templates. |
| **UC3.3** | Access Awareness | User clicks on the awareness button and is directed to a page with information about cyber attacks. | System displays information regarding cyber threats and attacks. |
| **UC4.1** | View User Profile Dropdown | User clicks on the profile icon in the navbar and sees options like account settings, upgrade plan, and logout. | System displays the dropdown menu with available options. |
| **UC4.2** | Account Settings | User selects "Account Settings" to reset password or change email. | System navigates to the settings page where the user can update their info. |
| **UC4.3** | Upgrade Plan | User clicks on "Upgrade Plan" to purchase or change the service plan. | System redirects the user to the plan upgrade page. |
| **UC4.4** | Logout | User clicks "Logout" to exit the platform. | System logs the user out and redirects them to the homepage. |
| **UC5.1** | View and Edit Questionnaire Template | User selects a questionnaire template, answers the questions, and receives a result with security analysis. | System analyzes the answers and generates a security risk analysis report. |
| **UC5.2** | Create a New Project | User clicks on "Create Project" to start a new project. | System creates a new project and makes it available for management. |
| **UC5.3** | View or Share Template | User views their saved or starred template and shares it with others. | System allows the user to share or collaborate on the selected template. |
| **UC5.4** | Save and Star Templates | User selects and stars a template to easily access later. | System saves or stars the template for future easy access. |
| **UC6.1** | View Dashboard | User clicks on the "Behaviorance-I" logo to navigate to their dashboard. | System redirects the user to the dashboard where they can see templates, projects, and actions. |

### **Alternative Courses**

1.If the behavior data entered is wrong

**System Response:** The system identifies the error and displays an error message, requesting the admin to correct the data.

**Alternative Action:** The system provides a warning message, requesting the admin to correct the data, so the process can continue without errors.

2.If the admin cannot make a decision based on the report

**System Response:** The system offers the admin the opportunity to ask for more information, for example, asking for specific information on the report.

**Alternative Action:** The admin can ask the system for more information or a clearer breakdown to help make a decision.

3.If the admin encounters an issue while logging the behavior assessment

**System Response:** The system shows an error message like "Unable to log assessment" when there's an issue.

**Alternative Action:** The system automatically saves the assessment and shows the admin an error message so they know that something went wrong, or it might let the admin try again

4.If the final report cannot be generated

Alternative Action: The admin may generate the report manually.

5.If the compliance score can't be updated

**System Response:** This means the system will inform the admin that the compliance score failed to update

**Alternative Action:** The admin may make manual changes so the records from the system update

6.If the final report fails to generate

**System Response:** The system fails to generate the final report and notifies the admin.

Alternative Action: The admin is notified and presented with an option to request help or allow the system to retry generating the report automatically.

7.If the user does not receive the notification about the outcome

**System Response:** The system fails to send the notification to the user.

**Alternative Action:** The admin may send a notice to the user or the system will keep trying sending the notice until it is sent.

# Non - Functional Requirements

## Performance Requirements

Performance requirements ensure that your application functions efficiently and responds promptly to user interactions and system operations related to the **Behaviorance-I** web application platform. Specific performance requirements for your project may include:

* **Response Time:** The platform should provide real-time or near-real-time feedback on employee behavior and security risk predictions, ensuring that users can act on insights immediately.
* **Scalability:** The system must be able to handle a large number of users (employees) concurrently without significant degradation in performance. It should support scaling to enterprise-level usage, particularly during peak periods.

## **Safety Requirements**

Safety requirements ensure that the web application platform operates securely to protect users' personal information and ensure reliable functionality. Specific safety requirements for my project may include:

* **Data Integrity:** The platform must ensure the integrity of the collected data, preventing unauthorized modifications during transmission or storage.
* **User Safety:** Measures must be in place to ensure the safety of personal information related to user behavioral profiles. These data should not expose individuals to any form of risk, whether physical, psychological, or otherwise.

## **Security Requirements**

Security requirements protect the web application platform against unauthorized access, data breaches, and ensure the integrity of user interactions. Specific security requirements for my project may include:

* **Authentication:** The platform must require secure Multi-factor authentication for users, especially administrators and other privileged users.
* **Data Encryption:** means securing all collected data, such as behavioral profiles and personal information. It will also provide protection for the data if it is transferred or stored within the system.

## **Reliability Requirements**

Reliability requirements make sure the web application platform operates without failure or disruption. Specific reliability requirements for my project may include:

* **Uptime**: The system should ensure a minimum uptime of 99.9%, meaning that it is available and working for the users at all times, except for scheduled maintenance.
* **Backup and Recovery**: The platform should include automated backups to prevent data loss. In case of a system failure, the platform must have a disaster recovery plan in place to restore functionality within 1-2 hour.

## **Usability Requirements**

Usability requirements ensure that the web application platform is intuitive and easy to use for customers engaged in the Specific usability requirements for my project may include:

* **Intuitive Interface:** The user interface is also supposed to be simple, intuitive, not only for end users (employees), but also for the administrators. Non-technical users must not need much training so that they may easily interact with this platform.

## **Supportability Requirements**

Supportability requirements ensure that the web application is maintainable, upgradable, and scalable over its lifecycle. Specific supportability requirements for my project may include:

* **System Monitoring and Diagnostics**: It should have features to monitor system performance, identify issues, and throw alarms to the technical support teams.
* **Maintenance:** The system must be easy to maintain.

## **User Documentation**

**Administrator Documentation:**

There will be an in-depth user guide for the system administrators detailing how to get the platform set up, the configuration of system settings, and troubleshooting and maintaining the system. This will help ensure that the Behaviorance-I platform runs with minimal disruptions.

**End-User Documentation:**

Employee guides will be developed in easy-to-understand language to allow employees to engage with the platform effectively. It will include step-by-step instructions on:

Login and access the system

Navigate through the behavior analysis features

Complete security assessments and questionnaires

Interpret the results of behavior analysis

Understand and follow security recommendations based on their behavior

**Troubleshooting and FAQs:**

The documentation will cover common issues that end-users or administrators may encounter. This includes:

How to resolve login issues

What to do if the system fails to generate reports or display results

Solutions to connectivity or integration issues

This list is designed as a FAQ, meaning users will quickly know how to fix the most common problems themselves.

# References

# 1. Kannelønning, K. and Katsikas, S.K. (2023) ‘A systematic literature review of how cybersecurity-related behavior has been assessed’, Information & Computer Security, 31(4), pp. 463–477. Available at: https://doi.org/10.1108/ICS-08-2022-0139.

# 2. Almansoori, A., Al-Emran, M. and Shaalan, K. (2023) ‘Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories’, Applied Sciences, 13(9), p. 5700. Available at: <https://doi.org/10.3390/app13095700>.

# 3. Rohan, R. et al. (2023) ‘A systematic literature review of cybersecurity scales assessing information security awareness’, Heliyon, 9(3). Available at: <https://doi.org/10.1016/j.heliyon.2023.e14234>.

# 4. Khan, N.F. et al. (2022) ‘The cybersecurity behavioral research: A tertiary study’, Computers & Security, 120, p. 102826. Available at: <https://doi.org/10.1016/j.cose.2022.102826>.

# 5. Rohan, R. et al. (2021) ‘Understanding of Human Factors in Cybersecurity: A Systematic Literature Review’, in 2021 International Conference on Computational Performance Evaluation (ComPE). IEEE, pp. 133–140. Available at: <https://doi.org/10.1109/ComPE53109.2021.9752358>

# 6. Rahman, T. et al. (2021) ‘Human Factors in Cybersecurity: A Scoping Review’, ACM International Conference Proceeding Series [Preprint]. Available at: https://doi.org/10.1145/3468784.3468789.

# 7. Maalem, A. et al. (2020) ‘Review and insight on the behavioral aspects of cybersecurity’, Cybersecurity, 3(1), p. 10. Available at: https://doi.org/10.1186/s42400-020-00050-w.