Software Requirements Specification

for

Insurance Workflow Automation Software, Release 1.0

Version 1.2

Prepared by
Gautham P Atreyas - PES1UG21CS206,
Gagan H R - PES1UG21CS196,
Ganesh Mayya K - PES1UG21CS198,
Sathvik H D - PES1UG21CS212

Benchmen

September 15, 2023

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Benchmen	15-09-2023	Initial draft	1.0
Benchmen	11-09-2023	Filled TDB fields	1.1
Benchmen	21-11-2023	Modified 4.5, added 4.6	1.2
Benchmen	21-11-223	Modified 4.1, added 4.7, 4.8	1.3

1. Introduction

1.1 Purpose

The requirements for developing Insurance Workflow Automation Software (IWAS) are outlined in this SRS document. IWAS is an automation technology that has been carefully designed to transform insurance operations of leading insurance service providers. Its primary goal is to bring about operational excellence by streamlining insurance procedures, increasing effectiveness, and raising the bar for all aspects of customer service.

1.2 Document Conventions

Priority Assignment:
The following priority levels are used to designate the importance of requirements and features:

Priority = High: Indicates that the requirement is critical to the system's core functionality, and its implementation is essential for the successful deployment of the software.

Priority = Medium: Denotes requirements that are important but may not be critical for the initial release. They can be considered for implementation after high-priority requirements are addressed.

Priority = Low: Designates requirements that are nice to have but are not critical for the core functionality. These requirements may be considered for future enhancements or updates.

Numbering convention:
Section Level 1: Numbered with whole numbers (e.g., 1, 2, 3, ...)
Subsection Level 2: Numbered as a decimal of the section number (e.g., 1.1, 1.2, 2.1, ...)

Bullet points are used for lists of items, options, or features. Numbered lists are used for step-by-step procedures or sequences.

1.3 Intended Audience and Reading Suggestions

The intended audience for this document includes various stakeholders within insurance companies and related organisations. Within insurance companies, the following individuals will have the most use for IWAS:

- Underwriters: Individuals responsible for assessing risk and pricing insurance policies.
- Claim Adjusters: Professionals who investigate and settle insurance claims.
- Sales Executives: They carry out the following tasks:
    - Sell insurance policies to customers.
    - Handle customer inquiries and requests.

1.4 Product Scope

Under this subsection, we outline the boundaries and objectives of the software solution to IWAS. We define what the software will encompass, its features, and its intended functionality.

1. Policy Management:
    a. Creation and maintenance of insurance policies.
    b. Policy underwriting and risk assessment automation.
    c. Policy renewal and endorsement management.
    d. Premium calculation and billing automation.
    e. Policy document generation and distribution.

2. Claims Processing:
    a. Digital document storage and retrieval.
    b. Automated document indexing and categorization.
    c. Secure access control and permissions management.

3. User Access and Security:
    a. Role-based access control.
    b. Data encryption and security protocols.
    c. Authentication and multi-factor authentication.
    d. User activity monitoring and logging.
    e. Disaster recovery and data backup features.

4. Integration and Data Exchanges:
    a. Integration with external data sources (e.g., credit bureaus, government databases).
    b. API support for connecting with third-party services and partners.
    c. Data import/export capabilities.

1.5 References

RF-1: European Parliament, *General Data Protection Regulation*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

RF-2: Paswan, Ram. *Consumer Protection Act, 2019*.

RF-3: Benchmen, *IWAS Web Application User Interface Standard, Version 1.0*.

2. Overall Description

2.1 Product Perspective

The Insurance Workflow Automation System is a new software solution designed to streamline and modernise the existing manual, repetitive, paper-based processes involved in insurance related tasks within an organisation. The software empowers insurance organisations to streamline workflows, reduce errors, and adapt swiftly to changing market dynamics. The context diagram in Figure 1 illustrates the external entities and system interfaces for release 1.0.
This system will undergo multiple releases and enhancements to improve insurance operations progressively.

2.2 Product Functions

PF-1: The IWAS shall provide an interface for Customers to purchase policies through furnishing necessary details and documents.

PF-2: The IWAS shall provide an interface for Customers to claim their policies and provide necessary documents and proof for the same.

PF-3: The IWAS shall provide an interface for Sales Executives to track customer support requests, submit new insurance applications, manage clients and submit claim requests on client's behalf.

PF-4: The IWAS shall provide mechanisms for Insurance Underwriters, Claim Adjusters, Document Verifiers and Insurance Appraisers to carry out approvals or rejections on claim requests by customers.

2.3 User Classes and Characteristics

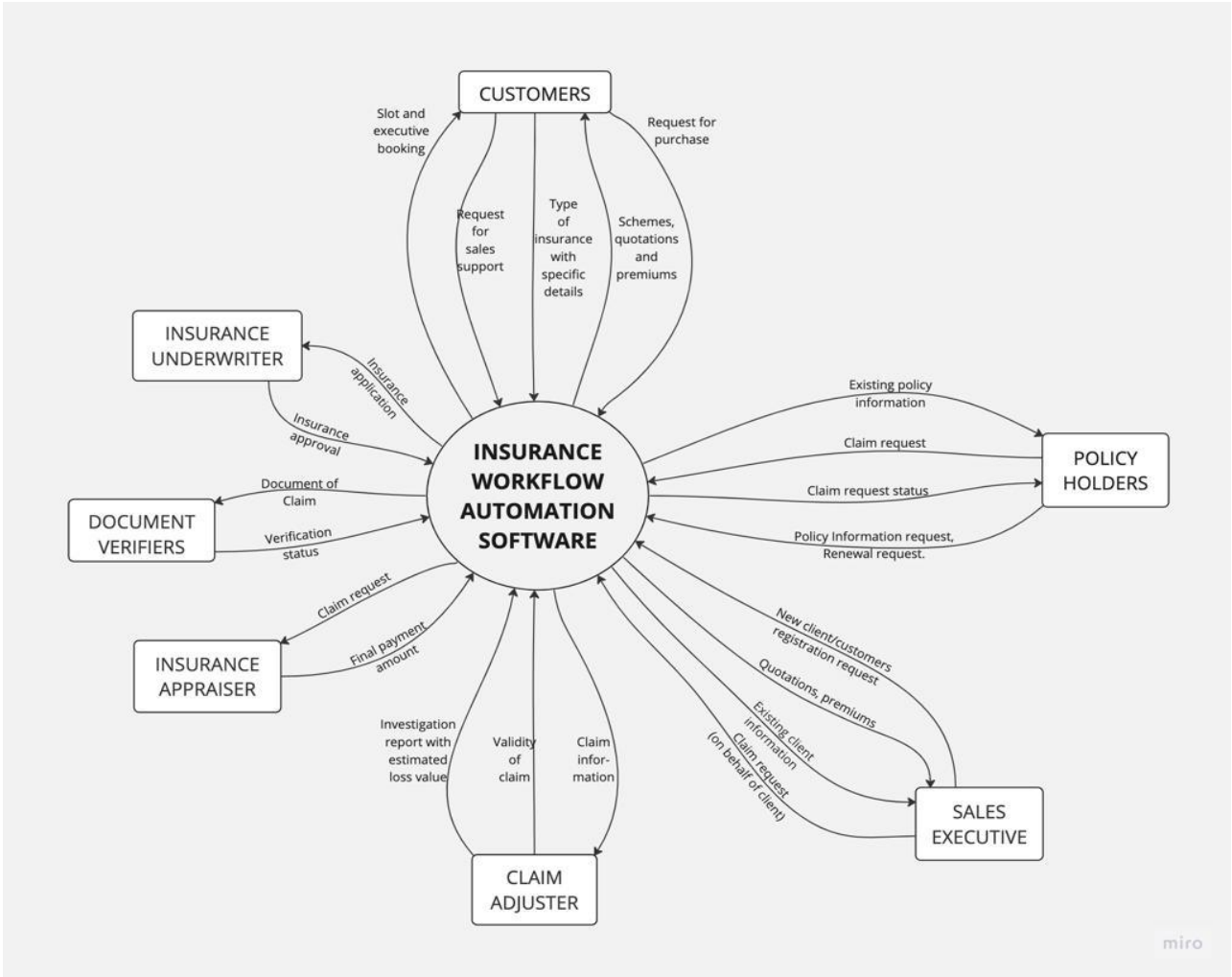

Figure 1 : *Context diagram for Insurance Workflow Automation Software v1.0*

Customer Insurance customers, often referred to as policy holders or policy buyers, are the lifeblood of the insurance industry. They are individuals, families, and businesses

	seeking financial protection for potential risks.
Administrator	Administrators are individuals within the corporate structure who are responsible for creating, modifying and deleting user accounts and data. They control the access of all the users of the IWAS.
Sales Executive	A Sales Executive sells the company's insurance products and services to potential customers or clients. They provide insurance quotations to clients on request. They keep track of all the existing clients, provide insurance support on policyholder requests, and submit claim requests to the IWAS and forwarded to the Claim Adjuster on behalf of the client.
Claim Adjuster	A claim adjuster assesses and evaluates the insurance claims at the preliminary stage by analysing the policyholder information, witnesses, and other document sources and determines the validity and extent of the claim. They interpret insurance policies to determine if the claim falls within the coverage given by the policy. The adjuster submits an investigation report along with an estimated loss.
Document Verifier	Document verifier validates and ensures that all policy and policyholder related documents are accurate, valid and compliant with the company’s guidelines and industry standards. They accept or flag the documents. Documents related to claims, licences, and other key documents are validated as part of the verification process.
Insurance Appraiser	Insurance Appraiser assesses the value of assets (property, vehicle, etc) for the purpose of claim settlements. They process the preliminary report by the claim adjuster and document verifier, perform further investigations and negotiations on the claim and cost of loss or damage. They submit the final payment settlement amount to IWAS.
Insurance Underwriter	Insurance underwriters evaluate risks, determine coverage and premium rates for insurance policies. They have the authority to approve or decline the insurance applications or modify the coverage and premiums to adjust risks. They also assess policy renewals to approve continuation of coverage.

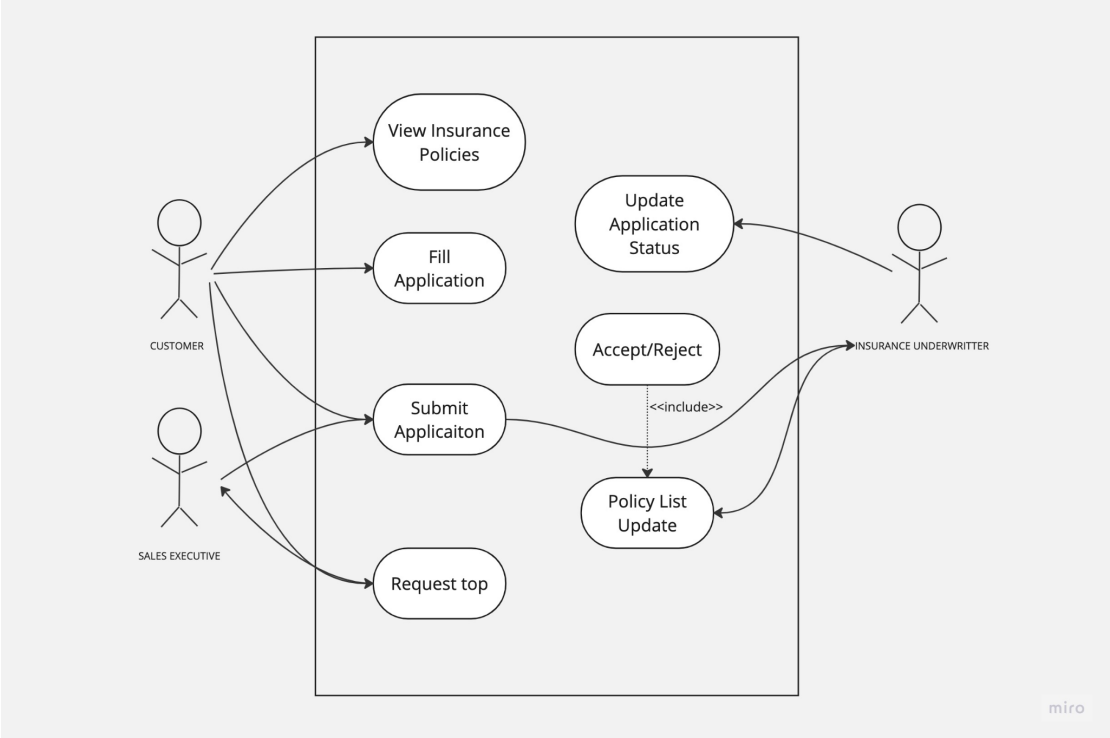

Figure 2 : *Use Case Diagram for Policy Purchase System*

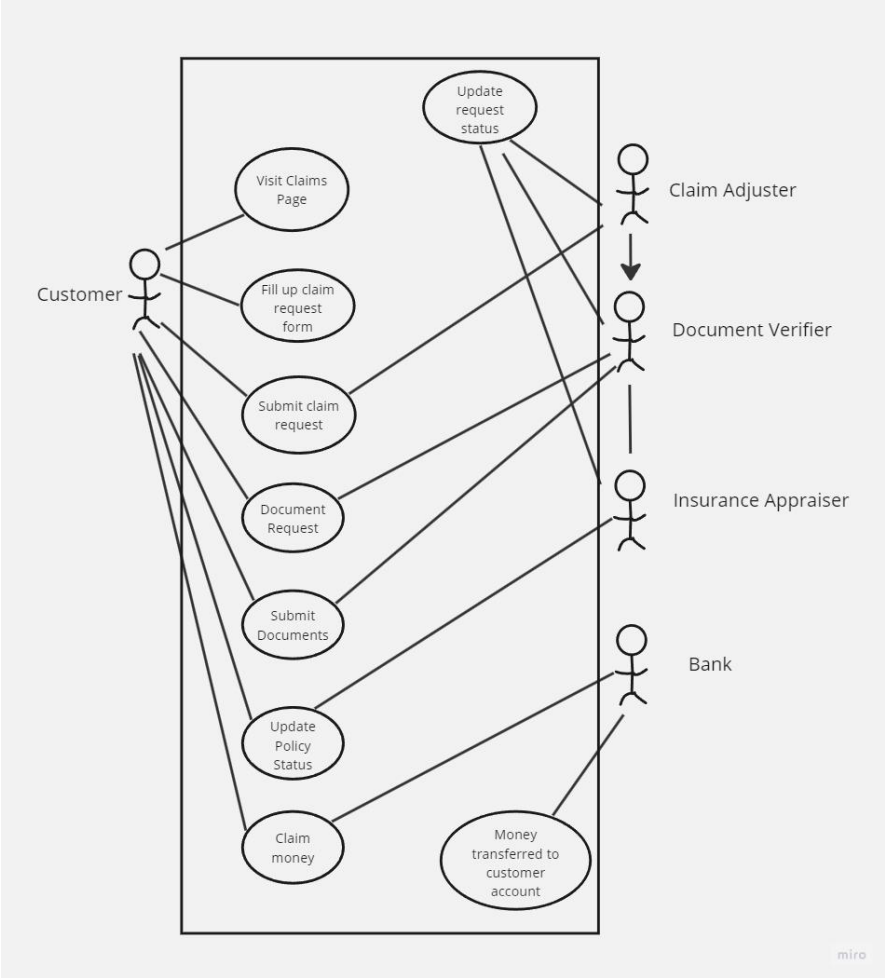

Figure 3 : *Use case diagram for Policy Claim System*

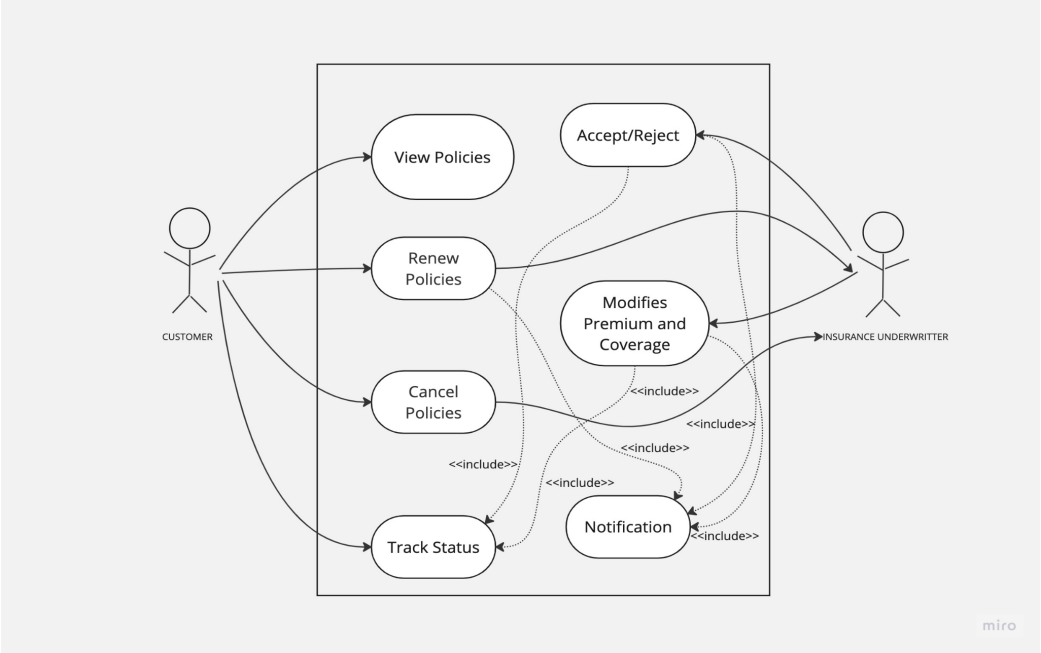

Figure 4 : *Use Case diagram for Policy Management System*

2.4 Operating Environment

OE-1: The IWAS shall be accessible on all modern Chromium and Firefox based browsers. The specific versions of browsers are listed below.

OE-1.1: Google Chrome: Version 64 and above

OE-1.2: Microsoft Edge: Version 79 and above

OE-1.3: Apple Safari: Version 12 and above

OE-1.4: Brave: Version 1.05 and above

OE-1.5: Mozilla Firefox: Version 58 and above

OE-2: The IWAS shall have support only for laptops and pc devices. It shall not have support for other computing devices such as mobile phones.

OE-3: The IWAS shall operate on a server running CentOS 8 and approved versions of Nginx.

2.5 Design and Implementation Constraints

DI-1: The IWAS server shall run on a system with a memory of 32 GB and a CPU with 16 cores.

DI-2: The IWAS shall not use more than 1 GB memory on the client system.

DI-3: The colour scheme of all the component shall have a minimum contrast score of

7, as specified in *Realtime Colors*

DI-4: The IWAS shall use PostgreSQL database for structured data and MongoDB for unstructured data.

DI-5: The frontend interface code shall be written in HTML 5.0 and Typescript 5.2.2.

DI-6: The backend server code shall be written in Python 3.11.

2.6 User Documentation

UD-1: The ‘Documentation’ component shall provide an online hierarchical help system that describes and illustrates all system functions. This component shall not be visible to the Customer.

UD-2: The IWAS comes bundled with ‘Readme’ and ‘User Manual’ documents which shall cover all the details of the system workings required by the Admin.

2.7 Assumptions and Dependencies

AD-1: UIDAI API for Aadhaar number authentication via e-KYC will be utilised for user registration.

AD-2: OpenAI APIs for building a chatbot for customer services and FAQs.

AD-3: API Setu (by the Government of India) for APIs to access driving licence and vehicle registration documents.

3. External Interface Requirements

3.1 User Interfaces

UI-1: The IWAS shall consist of a single webpage, which can be navigated using a mouse or a keyboard. All the components of the application are described in the RF-3

UI-2: The webpage shall consist of a navigation bar at the top. The content of the navigation bar is described in the RF-3

UI-3: Each component shall follow a consistent font style and a colour scheme which is described in RF-3

UI-4: The ‘Dashboard’ component shall consist of different sub-components based on the role of the user.

UI-4.1: The Customer shall be able to track all his purchased policies and requests in the ‘Dashboard’ component..

UI-4.2: The Admin shall be able to search for specific user ids and view their account details.

UI-4.3: The Insurance_Underwriter, Claim_Adjuster, Document_Verifier and Insurance_Appraiser shall be able to view and manage all the respective requests.

UI-4.4: The Sales_Executive will be able to view Customer details and status of requests allotted to him.

UI-5: The ‘Dashboard’ component shall consist of an AI Chatbot at the bottom right corner, which will assist the user with FAQs.

UI-6: Every input field in a form shall have a ‘?’ symbol placed to the right of the label. When the symbol is hovered, a brief description of the input field, consisting of less than 50 words shall appear to the right of the symbol.

UI-7: Every form shall have a confirmation pop-up when the user clicks on the ‘Submit’ button.

UI-8: Every error message shall be classified into two categories based on priority. Client side errors shall be classified as ‘Low-priority’ and server side errors shall be classified as ‘High-priority’.

UI-8.1: ‘Low-priority’ errors shall be displayed as a pop-up at the top of the screen. ‘High-priority’ errors shall prevent the user from accessing the application until the server has been restarted.

3.2 Hardware Interfaces

The IWAS shall not consist of any hardware components.

3.3 Software Interfaces

SI-1: BenchBank User Authentication System Version 2.3

SI-1.1: When creating a new account, the *AADHAAR* number and the phone number shall be verified using the components specified in Section 2.7

SI-1.2: User account details shall be stored in a NoSQL database. The password, AADHAAR number and phone number shall be hashed before storing.

SI-1.3: Upon successful account creation, a unique `Account_ID` shall be assigned to the account. All accounts shall have a default privilege level of ‘Customer’.

SI-1.4: On login, the provided credentials shall be checked against the values stored in the database. Only upon a successful login shall the user be granted access to components other than the `Home`, `Support` and `About` components. On an

unsuccessful login, the user shall be denied access.

SI-1.5: The number of consecutive unsuccessful login attempts shall be tracked for each IP address. The IP shall be blocked for a period of 1 hour if the number crosses a modifiable threshold (default threshold shall be set to 5 attempts). Only the Admin can modify the threshold.

SI-1.6: The user shall have the option to reset the password of their account, by using either their registered email or phone number.

SI-2: BenchBank Customer Service AI Chatbot Version 3.1

SI-2.1: The chatbot shall have a prompt to type in questions, along with a list of the most popular questions.

SI-2.2: This service shall be built using OpenAI APIs for Large Language Models (LLMs), as mentioned in Section 2.7.

SI-2.3: The chatbot will provide responses within 2 seconds to common queries by accessing a knowledge base stored in memory.

SI-2.4: The chatbot will provide responses within 15 seconds to queries which are not in the knowledge base.

3.4 Communications Interfaces

CI-1: The IWAS shall send API queries to UIDAI to verify AADHAAR number and phone number while creating an account.

CI-2: The IWAS shall send an OTP to the Customer’s email while purchasing an insurance policy.

CI-3: The IWAS shall send an OTP to the Customer’s email while initiating a claim.

CI-4: The IWAS shall send monthly notification emails to the Customer regarding the status of insurance policies the Customer owns.

CI-5: The IWAS shall send renewal notification emails and SMS to the Customer regarding a policy that will expire in 5 days.

4. System Features

4.1 Policy Purchase System

4.1.1 Description and Priority

A verified Customer may purchase various types of insurance policies offered. The Policy Purchase System handles the process of receiving purchase requests, displaying available policies, and managing the policy purchase routers. Priority = High.

4.1.2 Stimulus/Response Sequences

Stimulus: Customer visits Purchase Policy component.

Response: System queries the database manager and retrieves a list of insurance policies and their details.

Stimulus: Customer picks a particular type of policy from the list, fills the requirements for that policy and submits a purchase request.

Response: System validates the purchase request, and pushes it to an available purchase router. The purchase request gets added to the Policy Manager.

Stimulus: The purchase router pops the purchase request from the router.

Response: The policy system sends a notification to the customer about the purchase request status.

4.1.3 Functional Requirements

FR-1:	The system shall be in charge of creating routers and distributing the purchase requests amongst the routers
FR-2:	Form validation shall be carried out on the details entered by the customer into the policy requirements form.
FR-2.1:	No input field can be empty.
FR-3::	The system shall display a list of available insurance policies to the customer.
FR-4::	The system shall apply the Round Robin algorithm to select a policy purchase router based on the current load of each router.
FR-5:	The system shall retrieve a list of Document Verifiers and Approvers and distribute them amongst the purchase routers.
FR-6:	The system shall store user submitted documents in a storage bucket, and return the url of the document.

4.2 Policy Claim System

4.2.1 Description and Priority

A verified Customer may choose to claim their purchased policies before the expiration of the policy. The claim request gets routed multiple times as it gets validated at multiple stages by the respective roles. The transaction gets audited and the claim request is updated in the Customer’s ‘Dashboard’ at every stage. Priority = High.

4.2.2 Stimulus/Response Sequences

Stimulus: Customer requests to claim their policy. The Customer will not be able to cancel a claim request once it has been initiated.

Response: System sends the claim request to a Claim Adjuster who validates. The claim request gets tracked on the Customer's Dashboard.

Stimulus: The Claim Adjuster decides to either approve or reject the claim request.

Response: If the Claim Adjuster approves the request, the request is routed to a Document Verifier. The Customer is appointed a Sales Executive, who will act as the human interface for the Customer.

Stimulus: The Document Verifier requests the necessary documents of the Customer.

Response: System sends a notification to the Customer and updates the claim request in their 'Dashboard' to facilitate submission of documents listed by the Document Verifier.

Stimulus: Customer submits the required documents.

Response: System updates the claim request in the Document Verifier's 'Dashboard'.

Stimulus: The Document Verifier decides to either approve or reject the claim request.

Response: If the Document Verifier approves the request, the request is routed to an Insurance Appraiser.

Stimulus: The Insurance Appraiser decides to either approve or reject the claim request.

Response: If the Insurance Appraiser approves the request, the claimed money is transferred to the Customer's BenchBank account. The policy of the Customer is updated.

4.2.3 Functional Requirements

FR-1:	The button to cancel a claim request shall be disabled once the request has been initiated.
FR-2:	An interface will be provided to allow the customer to upload documents in .png, .jpg or .pdf format from local storage, cloud storage, or DigiLocker.
FR-3:	All the operations are atomic.
FR-4:	Once the request is approved by the Insurance Appraiser, the customer will be notified via both email and SMS.
FR-5:	A service will be provided to the user to check the status of the request, with a graphical representation of the completed stages and stages yet to be completed.

4.3 Policy Manager

4.3.1 Description and Priority

A verified Customer shall be able to view, renew and cancel all the policies they have purchased in the ‘Dashboard’ component. The Customer shall receive notifications about policies which will expire in 5 days. The Customer shall be able to track ongoing purchase and claim requests. Priority = High.

4.3.2 Stimulus/Response Sequences

Stimulus: Customer requests to renew a policy.

Response: System queries the Customer for details of renewal amount and renewal time, and routes the renewal request to the Insurance Underwriter.

Stimulus: Customer requests to cancel a policy.

Response: System queries the penalty amount and displays it to the Customer.

Stimulus: Customer chooses to go ahead with the cancellation.

Response: System handles the cancellation, deducts the penalty amount and deposits the remaining amount in the Customer’s BenchBank amount.

4.3.3 Functional Requirements

FR-1:	Customers can view, renew, and cancel purchased policies from the 'Dashboard' component.
FR-2:	Customers receive notifications about policies expiring in 5 days.
FR-3:	Customers can track the status of ongoing policy purchase and claim requests.
FR-4:	Customers can customise how they receive notifications (email, SMS, etc.).
FR-5:	The system maintains an audit log of all policy-related actions.

4.4 Customer Support

4.4.1 Description and Priority

A verified Customer shall be able to use the AI chatbot for any queries. They also have the option to book an appointment with a Sales Executive. The Customer can contact a Sales Executive while purchasing a policy, and give them permission to track the purchase request as well. Priority = Medium.

4.4.2 Stimulus/Response Sequences

Stimulus: Customer initiates interaction with AI Chatbot for general queries

Response: System enables AI chatbot to greet the customer and offer assistance with their inquiries.

Stimulus: The Customer requests to book an appointment with a Sales Executive.

Response: System queries the preferred date and time information for the appointment and schedules it.

Stimulus: The Customer grants permission for the Sales Executive to track their purchase request.

Response: System grants access to necessary customer data and application tracking information to the Sales Executive.

Stimulus: The Customer denies permission for the Sales Executive to track their purchase request.

Response: System proceeds without granting permission to Sales Executive to track insurance application.

4.4.3 Functional Requirements

FR-1:	Users can query the AI chatbot.
FR-2:	Customers can schedule an appointment with a Sales Executive
FR-3:	Customers can initiate contact with a Sales Executive during the policy purchase process.
FR-4:	Customers can grant permission to Sales Executives to track their purchase requests.

4.5 React Web Manager

4.5.1 Description and Priority

All users shall be able to navigate through the components accessible by them using either a keyboard or a mouse. The system shall consist of a single-page application where components are rendered dynamically. The system shall consist of a global state store for maintaining JWT token, user id and user email.

4.5.2 Stimulus/Response Sequences

Stimulus: User hovers over a link.

Response: The link is highlighted.

Stimulus: User clicks on a link.

Response: System renders the associated component..

4.5.3 Functional Requirements

FR-1:	Users must be able to navigate components using both a keyboard and a mouse.
FR-2:	Each web page must include a top navigation bar with links to render components.
FR-3:	Interactive elements, such as navigation links and buttons, must provide visual feedback when hovered over or focused on.
FR-4:	Navigation links within the top bar must maintain a consistent structure across all components
FR-5:	The web page must be compatible with screen readers for users with visual impairments
FR-6:	User assistance options must be available for guiding users in keyboard and mouse navigation
FR-7:	Components shall have a separate sub-navigation bar for navigating through sub-components
FR-8:	A global state store shall maintain user email, user id, and the JWT token upon login
FR-9:	A pop-up form shall display at the centre of the screen upon clicking the Login button.
FR-10	The Login button shall be replaced by the Logout button when the user is logged in
FR-11	The application shall consist of only classless functional components.

4.6 Session Manager

4.6.1 Description and Priority

The session manager shall handle creating and verifying JWT tokens, login and signup, hashing and verifying passwords. It shall also handle creating protected routes in the backend server.

4.6.2 Stimulus/Response Sequences

Stimulus: Client request without a JWT token is received on a protected route

Response: The session manager responds with an error message stating that the token is missing or invalid

Stimulus: Client request with a valid JWT token is received on a protected route

Response: The session manager validates the JWT token and grants access to the protected route

4.6.3 Functional Requirements

FR-1:	The session manager shall create a unique JWT token for each user upon successful login.
FR-2:	The session manager shall verify the validity of JWT tokens before granting access to protected routes.
FR-3:	The session manager shall store and manage user information, including user ID and email, associated with the JWT token.
FR-4:	The session manager shall handle password hashing and verification using bcrypt during login and signup processes.
FR-5:	The session manager shall handle error conditions gracefully, providing informative error messages in case of invalid tokens, missing credentials, or other authentication failures.
FR-6:	The session manager shall handle error conditions gracefully, providing informative error messages in case of invalid tokens, missing credentials, or other authentication failures.
FR-7:	The session manager shall provide an interface for invalidating JWT tokens, such as upon logout or session inactivity.

4.7 Profile Manager

4.7.1 Description and Priority

The profile manager handles changing a limited number of user account information. The customers can change their email, password, phone number, occupation, employment status and employer name. The customer can also add more users to their account, with the necessary information to create an account, to fast track the purchase and claim of policies related to the other users.

4.7.2 Stimulus/Response Sequences

Stimulus: User clicks on the "Profile" link.

Response: The Account component is rendered, displaying the user's profile information.

Stimulus: User changes their email address in the profile form.

Response: The system validates the new email address for format and uniqueness. If

valid, an email verification link is sent to the new address.

Stimulus: User enters their current password and a new password in the password change form.

Response: The system validates the current password and updates the password if valid.

4.7.2 Functional Requirements

FR-1:	The Profile Manager shall allow users to update their email address, password, phone number, occupation, employment status, and employer name.
FR-2:	The Profile Manager shall validate the entered information during profile updates and ensure it adheres to the specified formats and constraints.
FR-3:	The Profile Manager shall implement email verification for changing email addresses to prevent unauthorised access.
FR-4:	The Profile Manager shall allow users to add new users to their account by providing the necessary information, including name, email, phone number, and occupation.
FR-5:	The Profile Manager shall validate the information provided for new users and it to the customer's account if valid.
FR-6:	The Profile Manager shall send an email notification to the new user with instructions on completing the registration process.

4.8 Policy Purchase Router

4.7.1 Description and Priority

The Policy Purchase Router receives purchase requests from the policy purchase system and handles the routing of the requests to the Document Verification and Policy Approval.

4.7.2 Stimulus/Response Sequences

Stimulus: The system receives a purchase request from the Policy Purchase System.

Response: The system routes it to the required employee if available, else stores it in a buffer.

4.7.3 Functional Requirements

FR-1:	The system should route a purchase request to the required employee based on the Round Robin algorithm. If the required employee is available, the system sends the request to them; otherwise, it stores the request in a buffer.
FR-2:	When the system determines that the purchase request requires document verification, it should send the request to the Document Verifier employee for processing.
FR-3:	If the purchase request requires approval, the system should send the request to the Policy Approval employee for processing.
FR-4:	After the purchase request has been processed by the Document Verifier and Approver, the system should send the final decision or information back to the Customer.
FR-5:	The system should allow the configuration of the maximum size of the buffer for storing purchase requests.
FR-6:	The system should perform cleanup activities, such as releasing assigned employees and handling any pending requests, when the router is being deleted or reset.
FR-7:	The system should preserve the state of the router, including the current positions of the Document Verifier and Approver pointers, to resume operations after a restart or failure.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

PR-1: The response time for all queries shall be within 10 seconds. If it exceeds 10 seconds, the user shall be notified of the delay.

PR-2: The application will be able to support up to 200 concurrent users.

PR-3: All static components shall render within 3 seconds.

5.2 Safety Requirements

SF-1: IWAS shall encrypt sensitive and private information of customers, including contact information, financial information, medical information and claims history before storing it in respective SQL databases.

SF-2: IWAS shall maintain a consistent and structured backup strategy to ensure the company’s critical data can be restored in the event of data loss or corruption.

SF-2.1: The backup process for non-critical information shall be scheduled during the first week of every month .

SF-2.2: The backup process for critical information and audit logs shall be scheduled at 0600 hours every day.

SF-2.3: Redundant storage media such as RAID arrays will be used to minimise the risk of data loss due to hardware failures.

SF-2.4: Backups will be stored in multiple physical and geographic locations to protect against physical disasters affecting the primary backup.

SF-2.5: A monitoring system shall be implemented to alert the company to backup failures or issues.

5.3 Security Requirements

SY-1: IWAS shall ensure that only valid users can access the data and services offered.

SY-1.1: Users can access the application only through a HTTPS connection

SY-1.2: Passwords shall be hashed using SHA-256 both client and server side.

SY-2: The IWAS shall authenticate users as described in SI-1. Users can opt for extra protection via two-step verification.

SY-2.1: On login, the provided credentials shall be checked against the values stored in the database.

SY-2.2: If two-step verification has been enabled, the user will get an additional prompt on their registered mobile phone for verification.

SY-3: The IWAS shall maintain audit logs to track all user activities.

SY-4: The IWAS shall provide Role-Based Access Control to provide restricted access to information to all individuals within a network according to their roles.

5.4 Software Quality Attributes

SQ-1: The IWAS shall be available to all users on the Internet at a 98% uptime between 0700 hours and 2100 hours.

SQ-2: All operations by the user shall be atomic.

SQ-3: The number of medium and high severity bugs shall be less than 20 and 5 respectively on release.

SQ-4: While filling a form, all the details shall get temporarily stored in local storage

of the client, after every 5 seconds.

5.5 Business Rules

BR-1: Customer : The privileges that the customer has are as follows:

BR-1.1: Customers can access only their own information, which includes policy information, premium payment history, claim status. They cannot access any information of other Customers.

BR-1.2: Customers are allowed to modify the settings and details of only their own accounts, such as login credentials, contact information, and privacy settings.

BR-1.3: The customer is allowed to read purchase and claim requests only once the relevant applications have been submitted.

BR-2: Administrators (referred to as Admin henceforth) : The privileges that the admin has are as follows:

BR-2.1: Admins are allowed to create, modify and delete user accounts within the software. This includes granting or revoking access to specific features or data based on user roles and permissions.

BR-2.2: Admins have full access to all data within the software. The sensitive and private data will be in a hashed format.

BR-2.3: Admins can view audit logs and track user activities within the software to monitor for any unauthorised or suspicious actions.

BR-3: Sales Executives: The privileges that the sales executive has are as follows:

BR-3.1: Sales Executives can access the policy details of their policyholder.

BR-3.2: Sales Executives can place claim requests on behalf of the policyholder.

BR-4: Claim Adjusters : The privileges that the claim adjuster has are as follows:

BR-4.1: Claim Adjusters can investigate insurance claims by accessing the policy details of the policyholders, submitted witnesses and submitted documents to determine the validity and extent of the claim.

BR-4.2: Claim Adjusters can submit an estimated claim amount to be covered for the claim.

BR-5: Document Verifiers : The privileges that the document verifier has are as follows:

BR-5.1: Document Verifiers can access all insurance-related documents, including policy applications, claims forms, and supporting documentation.

BR-5.2: Document Verifiers can identify and flag any discrepancies or non-compliance issues in documents.

BR-6: Insurance Appraisers : The privileges that the Insurance_Appraisers has are as follows:

BR-6.1: Insurance Appraisers can access the reports of the Claim adjuster and Document Verifiers

BR-6.2: Insurance Appraisers can modify the estimated amount submitted by the claim adjuster and submit the final amount covered for the claim, which is then paid to the policyholder.

BR-6.3: Insurance Appraisers can submit the final amount covered for the claim, which is used for claim settlement and documentation.

BR-7: Insurance Underwriters : The privileges that the insurance underwriter has are as follows:

BR-7.1: Insurance Underwriters can approve or decline the purchase requests based on a risk assessment report.

BR-7.2: Insurance Underwriters can modify the policy coverage limits, premium and tenure to adjust the risk levels associated with the application.

6. Other Requirements

OR-1: The IWAS shall conform with the General Data Protection Regulation as specified in RF-1.

OR-2: The IWAS shall conform with the Consumer Protection Act as specified in RF-2.

OR-3: System Requirements 4.4 and 4.5 shall be made into separate components, and made available for reuse.

OR-4: The IWAS application shall be available in the following languages: English, Kannada, Spanish, French and Mandarin.

OR-5: The IWAS application shall support transactions in the following currencies: U.S. dollar, Euro, Indian Rupee and Chinese Yuan.

Appendix A: Glossary

AD Assumption or Dependency

BR Business Rule

CI Communications Interface

DI Design or Implementation

FR Functional Requirement

OE	Operating Environment
OR	Other Requirement
PF	Product Function
PR	Performance Requirement
RF	Reference
SF	Safety Requirement
SI	Software Interface
SQ	Software Quality Attribute
SY	Security Requirement
UD	User Documentation
UI	User Interface

Appendix B: To Be Determined List

1. Table of contents page numbers