Risk Management Plan for:
Vrddhopasthaan : Senior Citizen Health & Reminder App

Version: *1.0*

Approval date: *29 March, 2025*

Risk Management Plan for *Vrddhopasthan: Senior Citizen Health and Reminder App*

DOCUMENT CONTROL PANEL		
File Name:	Vrddhopasthan : Senior Citizen Health and Reminder App	
File Location:	Github Repository	
Version Number:	1.0	
Created By:	Avilasha Goswami (2230162)	
	Deep Habiswashi (2230167)	
	Kaushiki Sarkar (2230177)	
	Soumyadeep Dutta (2230207)	
Reviewed By:		
Modified By:		
Approved By:		

Table of Contents

List of Tables

List of Figures

List of Acronyms and Abbreviations

SCHRA	Senior Citizen Health and Reminder App
RMP	Risk Management Plan
ROM	Rough Order of Magnitude

Risk Management Plan for *Vrrdhopasthan : Senior Citizen Health and Reminder App*

1 Scope

1.1 Purpose

This Risk Management Plan (RMP) establishes the process for implementing proactive risk management as part of the overall management of a Senior Citizen Health and Reminder App (SCHRA) project. The purpose of risk management is to identify potential problems before they occur, so that risk-handling activities may be planned and invoked as needed across the life of the project to mitigate adverse impacts on achieving objectives. Risk management is a continuous, forward-looking process that addresses issues that could endanger achievement of critical objectives and includes early and aggressive risk identification through the collaboration and involvement of relevant stakeholders. The risk management approach is tailored to effectively anticipate and mitigate the risks that have critical impact on project objectives. While technical issues are a primary concern both early on and throughout all project phases, risk management considers both internal and external sources for cost, schedule, and technical risk. Early and aggressive detection of risk is a SCHRA project objective because it is typically easier, less costly, and less disruptive to make changes and correct work efforts during the earlier, rather than later, phases of the project.

This document describes the process to:

- Identify risk events and risk owners
- Evaluate risks with respect to likelihood and consequences
- Assess the options for the risks and develop mitigation plans
- Track risk mitigation efforts
- Conduct periodic reassessments of project risks

The RMP should be updated as necessary and the identified risks will be tracked until they are retired.

2 Applicable Documents

2.1 Senior Citizen Health and Reminder App

2.1.1 SCHRA Project Documentation

The following documents are prepared as part of the project documentation:

- Project Management Plan: Defines project scope, objectives, scheduling, resources, and deliverables.
- Systems Engineering Management Plan: Covers system design, development, integration,

and validation methodologies.

- Software Development Plan: Details software lifecycle, architecture, coding standards, and technology stack.
- Configuration and Data Management Plan: Specifies data security, backup, version control, and configuration tracking.
- Quality Assurance Plan : Outlines testing methodologies, bug tracking, and performance evaluation.
- Statement of Work: Defines contractual obligations, milestones, deliverables, and acceptance criteria.

3 Definitions

This section defines any terms used in the RMP that may need clarification. Start with the following and tailor as necessary:

- **Risk** is a measure of the inability to achieve overall project objectives within defined cost, schedule, and technical constraints, and has two components: (1) the probability (or likelihood) of failing to achieve a particular outcome, and (2) the consequences of failing to achieve that outcome.
- **Risk Events** are those events within the project that, if unsuccessful, could result in problems in the development, production, and fielding of the system. Risk events should be defined to a level so that the risk and causes are understandable and can be accurately assessed in terms of likelihood/probability and consequences to establish the level of risk.
- **Technical Risk** is the uncertainty of achieving the program requirements for function, performance, and operability within the planned cost and schedule. Technical risks are associated with the ability of the system (i.e., product) design and production process to meet the level of performance necessary to satisfy the operational requirements. Failure to adequately address technical risk generally results in an inability to meet cost and schedule constraints while meeting technical requirements. Typical technical risk drivers include requirements, constraints, technology, and development approach.
- **Cost Risk** is the uncertainty in achieving the cost budget if none of the technical and none of the schedule risks should materialize. Cost risks are associated with the ability of the project to achieve its overall cost objectives. Two risk areas bearing on cost are (1) the risk that the cost estimates and objectives are inaccurate and/or unreasonable, and (2) the risk that project execution will not meet the cost objectives as a result of a failure to mitigate cost, schedule, and performance risks. Typical cost risk drivers include requirements, personnel availability, reuse, tools, and environment.
- **Schedule Risk** is the uncertainty of achieving the program schedule if none of the technical or cost risks should materialize. Schedule risks are those associated with the adequacy of the time estimated and allocated for the development, production, and fielding of the system. Two risk areas bearing on schedule risk are: (1) the risk that the schedule estimates and objectives are unrealistic and/or unreasonable, and (2) the risk that project execution will fall short of the schedule objectives as a result of failure to mitigate cost, schedule, and performance risks. Typical schedule risk drivers include requirements, need/delivery dates, technology availability, and resources.
- **Project Risk** is a risk that affects multiple project teams or spans the whole project

structure and is subject to scrutiny at the highest levels of project management. Project risk is associated with the overall status of the project. These risks are generally associated with the ability of the project to maintain political and other support. Failure to meet cost, schedule and technical objectives can produce project risk. In addition, external budget, priority and political considerations can produce project risk.

- **Risk Assessment** is the translation of risk data into information for evaluating risk and determining the likelihood and consequence. A risk assessment (or rating) is the value or level that is given to a risk event based on the analysis of the likelihood/probability and consequences of the event.
- **Risk Metrics** are measures used to indicate progress or achievement on risk events, for example, technical performance measures.

4 Project Summary

4.1 Project Scope

Our project covers a multi-platform mobile and web app that serves as a health reminder and management assistant.It includes integration with external medical databases and emergency services while ensuring usability for seniors (aged 60+).The project will provide features like personalized medication alerts, secure health record storage, appointment scheduling, and a dedicated emergency SOS function.

4.2 System Description

The SCHRA is a mobile and web-based application that provides holistic support for senior citizens by managing their health needs and mediating reminders for medications as well as emergency help. The system combines various features including automatic drug dose reminders and an SOS button and health record monitoring and caregiver account access so people stay safe and healthy.

As part of the risk management framework, the system is being analyzed for potential risks related to data security, system reliability, accessibility, and user engagement. Developed using a scalable cloud-based architecture, the system ensures real-time synchronization of health records and notifications. The system will undergo comprehensive testing to check its functional operations and performance capabilities and security measures to fulfill healthcare data regulations while minimizing failures.

5 Risk Management Strategy

To address identified risks, the following strategies will be applied:

- **Technical Risks**: Our application will use a cloud-based platform with self-adjusting functionality to handle changing user traffic patterns efficiently. Real-time health record updates will be possible through strong synchronization tools joined with emergency alert systems and reminder delivery.

- **Security Risks**: The system will safeguard its sensitive user health data using industry-setting protection methods which combine multi-factor authentication with data encryption together with strict access control measures. The system requires third-party security audits to detect weaknesses and enhance protection of its defenses on a regular basis.
- **Operational Risks**: The core functionality of the system will be reliably operated via continuous testing and redundancy backup methods which maintain the operation of medication reminders along with emergency SOS alerts together with caregiver monitoring. The application design includes intuitive user experience features such as large readable fonts together with contrasting design elements and voice command functionality for users who possess different abilities in using digital devices.
- **Project Risks**: Our project will employ specific compliance officers who will ensure full adherence to healthcare regulations as well as data protection laws throughout project execution. A development process with cycles will enable flexibility regarding feature improvements and system scalability and vendor transitions which help prevent interruptions to system operations.

6 Risk Management Process

The risk management process comprises four phases: identification, assessment, handling, and monitoring. (Refer to Figure A.4.1.) The following paragraphs describe the process used by the project to identify and manage its risks.

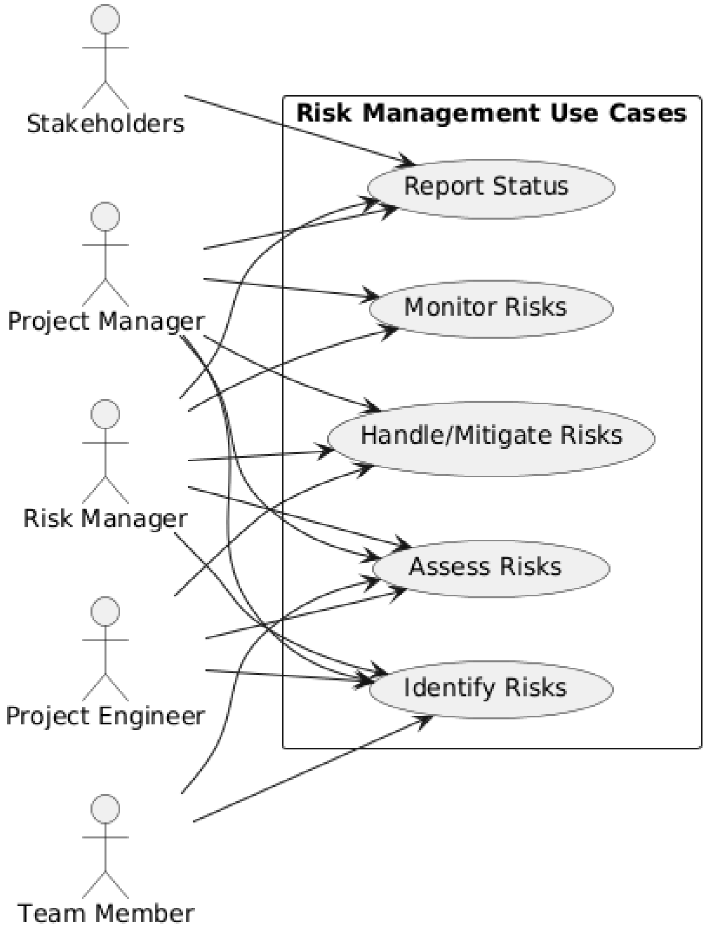

Figure A.4.1 – Risk Management Process

The following sections describe the suggested risk management process. Projects may tailor this process to best meet the needs of the project and/or satisfy the customer. The risk management process includes the following elements:

- **Risk Identification** – Examine all project elements in detail. Identify, describe, and document cost, schedule, technical, financial, and other risks. Begin the identification process during the capture phase and continue throughout the project life cycle.
- **Risk Assessment** – Evaluate the identified risks for probability of occurrence and potential impact. Estimate project exposure and establish risk-handling priorities. Qualitative assessments may be used as an initial filter but all medium and high risks must be assessed quantitatively. Express quantitative assessments (e.g., rough order of magnitude [ROM], range of impact, factored impact, etc.) in terms of dollars, time, and performance impact, as applicable.
- **Risk Handling** – Identify risk-handling options (i.e., mitigation, transfer, avoidance, assumption) and action plans, including contingency actions with implementation criteria and decision dates. Assign an owner to each risk and action plan. Ensure that risk handling plans document the criteria (i.e., observable, test, data, documentation) that justify the planned, sequential reduction of quantitative risk levels over time.

- **Risk Monitoring** – Track progress against action plans and established metrics to ensure timely completion of actions. Include action plans in the project integrated master schedule. Include risk name, description, identification date, owner, action plans, milestones, status, and contingency actions in the risk management database. Risk owners must provide status at least monthly.

6.1 Risk Identification

Risk identification is a critical process in the **Vrddhopasthaan** project, ensuring potential issues, vulnerabilities, and challenges are proactively identified and documented to minimize their impact on development, deployment, and user experience.

Methods for Identifying Risks

The project team employs multiple strategies to detect risks, including:

- **Analysis of app workflow and structure** to uncover potential risk areas.
- **Risk assessment reviews** to evaluate technical, operational, and compliance-related concerns.
- **Expert consultations** with healthcare professionals, caregivers, and technology specialists.
- **Review of past digital health applications** to identify recurring risks.
- **User feedback and pilot testing** to detect usability and functionality gaps.
- **Regulatory compliance checks** to ensure adherence to healthcare data privacy and security laws (e.g., HIPAA, GDPR).

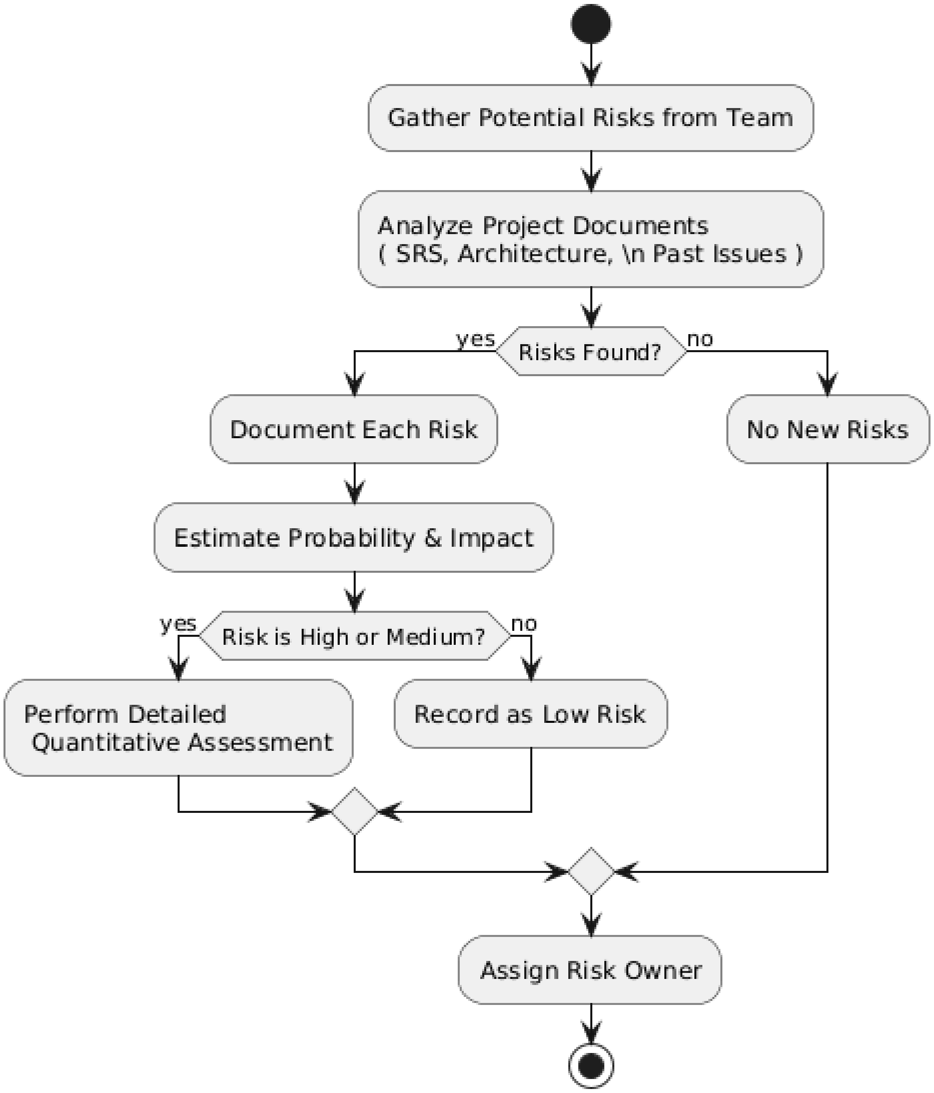

Fig 4.2 Risk Identification & Assessment

Key Risk Areas

Risk identification in **Vrddhopasthaan** spans multiple dimensions, including:

Technical Risks

- System crashes or **app downtime** affecting reminders and alerts.
- **Data security vulnerabilities** exposing sensitive health information.
- **Integration failures** with third-party health monitoring devices.
- **Scalability issues** as the user base grows.

Operational Risks

- **User errors** leading to missed medication reminders.
- **Lack of user engagement** causing app underutilization.
- **Complex UI/UX** making it difficult for seniors to navigate the app.

Regulatory & Compliance Risks

- **Failure to meet data privacy regulations** impacting legal compliance.
- **Insufficient accessibility standards**, making the app unusable for elderly users with disabilities.

Performance & Maintenance Risks

- **Bug accumulation** affecting app stability.
- **Delayed feature updates** leading to user dissatisfaction.
- **Failure of automated reminders** causing missed medication or appointments.

Early Risk Indicators

The project team should monitor signs that indicate potential risks, including:

- **User complaints or frequent support requests.**
- **Slow app performance or frequent crashes.**
- **Security breaches or privacy concerns reported.**
- **Low user retention and engagement metrics.**

By systematically identifying and addressing these risks, **Vrddhopasthaan** aims to ensure a **secure, reliable, and user-friendly experience** for senior citizens and their caregivers.

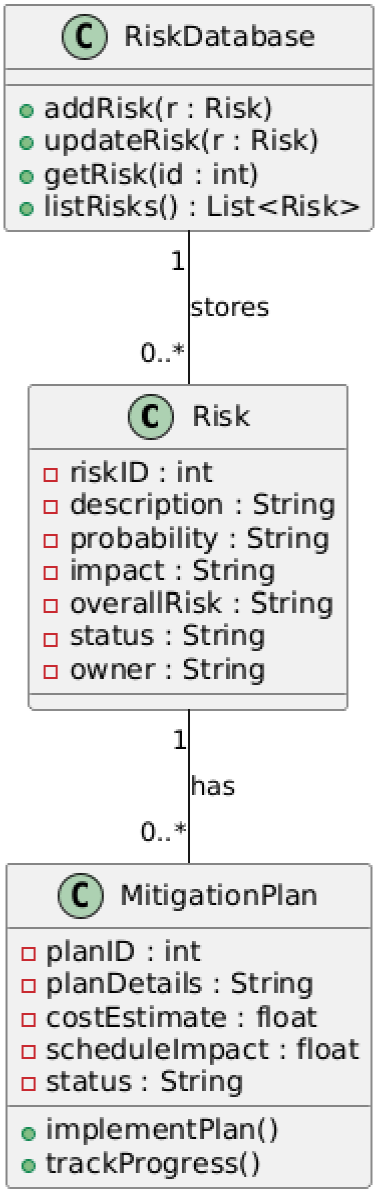

Fig 4.3 Risk Entities & Relationship

6.2 Risk Assessment

- **Regulatory Non-compliance**: Failure to meet healthcare data protection standards and regional medical regulations.
- **Limited Technical Resources**: Shortage of experienced personnel to handle AI, cloud infrastructure, and medical software complexities.
- **Funding Constraints**: Budget limitations affecting continuous feature development and maintenance.
- **Stakeholder Misalignment**: Risks due to conflicting requirements between medical professionals, caregivers, and end-users.

- **Vendor Lock-in**: Dependence on specific cloud providers or third-party service providers may lead to high switching costs.

Each risk is assessed based on:

- **Likelihood**: Probability of occurrence (Low, Medium, High).
- **Impact**: Consequences on project success (Low, Medium, High).

Table 1: Overall Project Risk Assessment

RISK CATEGORY	DESCRIPTION	LIKELIHOOD	IMPACT	MITIGATION STRATEGY
Technical Risks	Scalability issues as user base increases	High	High	Load Balancing, cloud auto-scaling
Technical Risks	AI model making incorrect health recommendation	Medium	High	Continuous training, human validation checks
Technical Risks	Compatibility issues with wearable devices	Medium	Medium	Thorough device testing and API standardization
Security Risks	Unauthorized access to health data	High	High	Implement MFA end-to-end encryption
Security Risks	Vulnerability in third-party APIs	Medium	High	Regular security audits, sandbox testing
Security Risks	Phishing attacks targeting elderly users	High	High	User education, security awareness training
Operational Risks	Failure in medication reminders	Medium	High	Redundant scheduling mechanisms, backup servers
Operational Risks	Poor UI/UX for elderly users	Medium	Medium	Extensive user testing, simplified navigation
Operational	Technical	Medium	High	24/7 helpline,

Risks	support delays			automated troubleshooting guides
Project Risks	Non-compliance with health data regulations	High	High	Regular audits, legal consultation
Project Risks	Non-compliance with health data regulations	Medium	High	Strategic partnerships, phased feature rollouts
Project Risks	Vendor lock-in with cloud service providers	High	Medium	Multi-cloud strategy, open-source alternatives

Once the risks are assessed, they are categorized into defined risk categories, providing a means of looking at risks according to their source or taxonomy, and are prioritized from 1 to n, 1 being the most effective area to which resources for mitigation are applied to achieve the greatest positive impact to the project.

6.3 Risk Handling

Risk handling is the process that identifies, evaluates, selects, and implements options to set risk at acceptable levels given project constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, and associated cost and schedule. The handling strategy is determined by the overall risk assessment rating as indicated below.

Table 2: Risk Handling Strategy

Overall Risk Assessment	**Handling Strategy**
High	The project manager and project engineer will monitor high-risk items **daily** until resolution. Risk owners will document and execute: - **Risk avoidance actions** (eliminating the source of risk where possible). - **Risk mitigation actions** (reducing the severity and impact of the risk). - **Contingency actions** (fallback plans to ensure project continuity).

Medium	Medium risks will be reviewed at regular intervals (e.g., **weekly or bi-weekly risk status meetings**). The handling strategy includes: - Implementation of mitigation strategies where possible. - Monitoring trends to prevent escalation to high-risk levels. - Adjustments based on new data and project progress.
Low	Low-risk items will be placed on a watchlist for ongoing monitoring. - These risks will be reviewed periodically to ensure they do not escalate. - No immediate action is required unless an escalation is triggered.

For each of these actions, measurable tracking criteria and decision dates are documented.

The most critical component of risk handling is the development of alternative courses of action, workarounds, and fallback positions, with a recommended course of action for each critical risk. Options for handling risks typically include alternatives such as the following:

- Risk avoidance by changing or lowering requirements, while still meeting user needs
- Risk control by taking active steps to minimize risks
- Risk transfer by reallocating design requirements to lower the risks
- Risk monitoring by watching and periodically reevaluating the risk for changes to the assigned risk parameters
- Risk acceptance by acknowledging the risk but not taking any action

6.4 Risk Monitoring

Risk monitoring ensures the continuous evaluation of identified risks and the effectiveness of risk-handling actions throughout the software development lifecycle. For *Vrddhopasthaan*, systematic tracking mechanisms will be implemented to assess the impact of risks on system performance, security, and user experience.

Key components of risk monitoring include:

- **Regular Risk Reviews**: Scheduled evaluations at each project milestone to reassess risk severity and update mitigation strategies.

- **Performance Metrics**: Monitoring system uptime, response time, and error rates to detect potential risks in real-time.

- **Incident Tracking**: Logging security breaches, data inconsistencies, and failure events for root cause analysis.

- **Resource Allocation**: Ensuring adequate personnel and tools are dedicated to resolving high-impact risks.

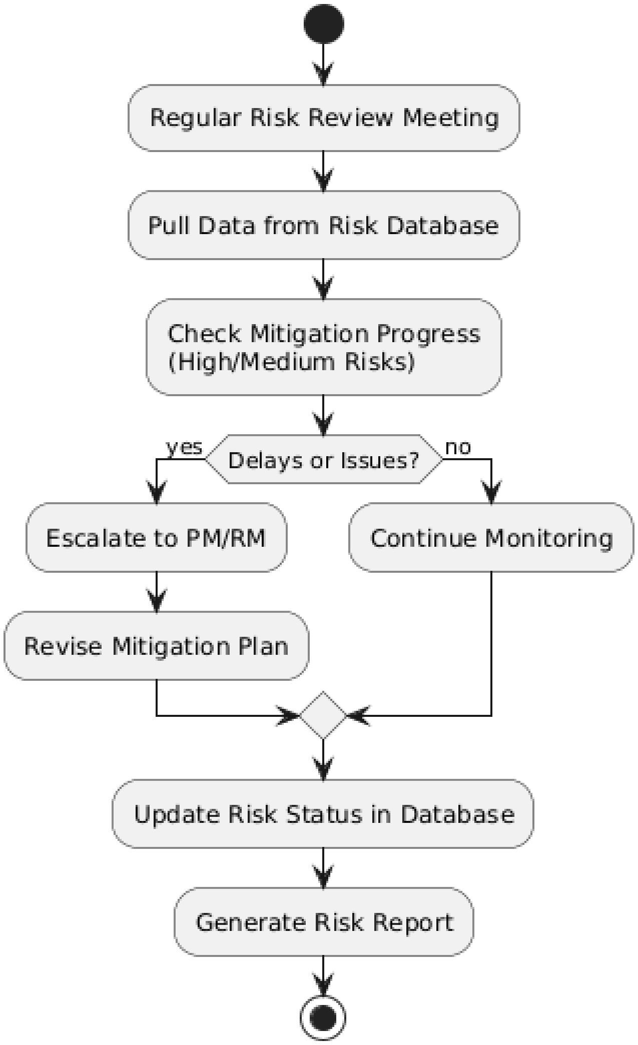

Fig 4.4 Risk Monitoring & Reporting

7 Risk Management Roles and Responsibilities

The risk management structure for *Vrddhopasthaan* includes key roles responsible for identifying, assessing, and mitigating risks.

Risk Management Oversight

- The **Project Manager** holds overall responsibility for risk management, ensuring integration with other project activities such as software development, security reviews, and compliance audits.

Risk Identification and Mitigation

- The **Technical Team** (developers, cloud engineers, and AI specialists) identifies software-related risks, including performance bottlenecks, data security threats, and integration failures.

- The **Compliance Officer** ensures that the app adheres to HIPAA, GDPR, and other relevant regulations.

Stakeholder Interfaces

- Risk management teams coordinate with **medical professionals**, **caregivers**, and **third-party service providers** to mitigate health-related risks and ensure seamless app usability.

- Collaboration with cloud service providers ensures continuous uptime and data security.

Organizational Chart Reference
A high-level organizational structure will be documented to illustrate risk ownership and responsibilities.

Training programs will be conducted to familiarize team members with risk management processes and mitigation strategies, ensuring an adaptive and proactive approach to risk handling.

7.1 Project Manager

The project manager has the overall responsibility for risk management on the project. The project manager may delegate this authority to another individual or team. If this is the case, state it here.

The project manager is responsible for the following:

- Establishes the Risk Management Plan (RMP).
- Allocates resources for risk mitigation.
- Approves and oversees high-risk mitigation plans.
- Reviews project risks and directs necessary actions.
- Communicates risk activities to the team.
- Identifies and addresses potential risks.

7.2 Risk Manager

The risk manager is the overall coordinator of the RMP. The risk manager is responsible for the following:

- Maintains the RMP and risk database.
- Reviews and evaluates risk control actions.
- Assesses cost implications of risk mitigation.

- Tracks risk reduction efforts.
- Provides risk management training.
- Prepares reports and risk briefings.

7.3 Project Engineer

The project engineer is responsible for the following:

- Identifies and documents risks.
- Gather risk assessment data.
- Ensures the RMP is feasible and complete.
- Monitors and reports engineering risk status.
- Ensures timely mitigation of technical risks.

7.4 Risk Individual Contributor

The **Risk Individual Contributor** is responsible for executing risk-related activities to ensure smooth operations and system security within ***Vrddhopasthaan***. Their responsibilities include:

- **Supporting risk identification** – Monitoring application performance, security vulnerabilities, and compliance risks.
- **Developing risk assessments** – Conducting detailed impact analyses for identified risks. **Supporting risk filtering** – Prioritizing risks based on severity, likelihood, and impact on users.
- **Developing and recording mitigation actions** – Implementing fixes and tracking risk mitigation progress.
- **Evaluating control actions** – Assessing whether implemented risk mitigation strategies are effective.
- **Identifying and assessing new risks** – Continuously analyzing potential new risks emerging from updates or third-party integrations.
- **Reporting risk status** – Providing updates during internal reviews and stakeholder meetings.

By performing these functions, risk contributors play a crucial role in minimizing disruptions and ensuring app reliability.

7.5 Customer and Stakeholder Participation

The **Vrddhopasthaan** project involves multiple stakeholders, including **senior citizens, caregivers, healthcare professionals, and regulatory bodies**. Their participation in risk management is essential to align the app's features with user needs and compliance requirements.

Key Areas of Stakeholder Involvement:

- **User Feedback Collection** – Customers report usability issues, security concerns, and system errors.

- **Healthcare Compliance Collaboration** – Ensuring adherence to HIPAA/GDPR data security requirements.
- **Risk Escalation Process** – Allowing caregivers and users to report high-impact risks (e.g., missed reminders, incorrect alerts).

7.6 Supplier Participation

Third-party suppliers (such as cloud service providers, API vendors, and security partners) play a critical role in risk management by ensuring reliable infrastructure, data security, and regulatory compliance.

Supplier Risk Management Responsibilities:

- **Cloud & Hosting Providers** – Ensuring uptime, backup solutions, and data protection.
- **Third-party API Vendors** – Maintaining secure and compliant integrations with external health databases.
- **Security Auditors** – Conducting periodic cybersecurity assessments and penetration testing.

The leadership team collaborates with suppliers to establish risk mitigation strategies, define responsibilities, and document agreements to ensure operational stability.

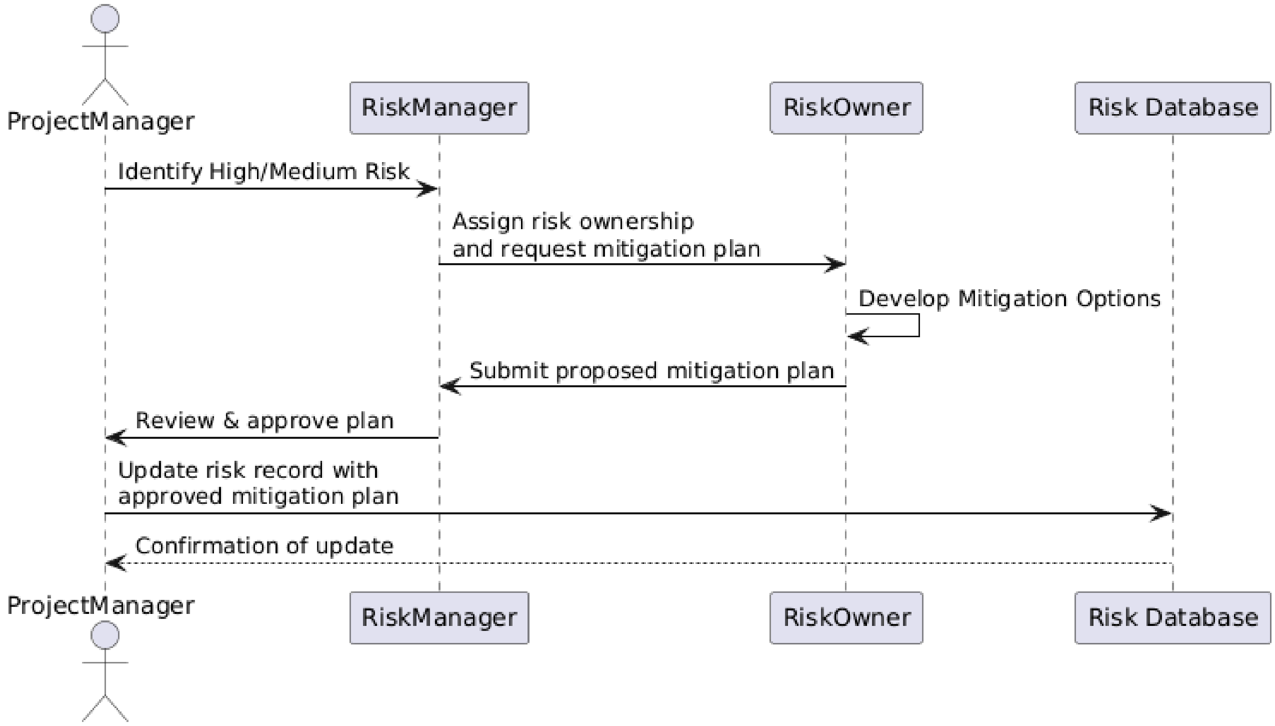

Fig 4.5 Risk Handling & Mitigation Process

8 Opportunity Management

In addition to mitigating risks, the **Vrddhopasthaan** risk management process also focuses on identifying **opportunities** to improve cost efficiency, enhance scheduling, and elevate service quality. Similar to risks, opportunities are systematically **identified, assessed, and prioritized** based on their potential impact on the project and user experience.

Unlike risks, which are mitigated or avoided, **opportunities should be exploited** to maximize their benefits. However, opportunities often require **proactive identification**, as they are less apparent than risks.

Opportunity Assessment Criteria

Each identified opportunity is evaluated using a **cost-benefit analysis** to ensure feasibility. The key criteria include:

- **Cost-to-benefit ratio** – Ensuring the opportunity yields significant advantages relative to its cost.
- **Technical feasibility** – Assessing whether implementation aligns with existing infrastructure.
- **User impact** – Evaluating how the opportunity enhances user experience and engagement.

Since exploiting opportunities carries inherent risks, the project team must ensure **stringent qualification criteria** before proceeding. Poorly executed opportunity exploitation plans could lead to wasted resources or unfulfilled expectations.

By carefully managing opportunities, **Vrddhopasthaan** can continually innovate and enhance its services for **senior citizens and caregivers**, ensuring better health outcomes and user satisfaction.

9 User Definitions

Version Number	Approved Date	Description of Change(s)	Created/ Modified By
1.0	29.03.2025		Avilasha Goswami, Deep Habiswashi, Kaushiki Sarkar, Soumyadeep Dutta