**Experiment No. 8: RMMM Plan Development**

### **Aim:**

To develop a Risk Management, Mitigation, and Monitoring (RMMM) plan for your software project.

### **Theory:**

Risk Management in software engineering involves identifying potential risks, assessing their impact, and developing strategies to manage them effectively. A comprehensive **RMMM Plan** ensures that risks are identified early, mitigated proactively, and monitored throughout the software development lifecycle.

**Key Components of RMMM Plan:**

1. **Risk Identification**
   * Identify potential risks that may impact project objectives, such as technical risks, resource risks, and schedule risks.
2. **Risk Assessment**
   * Assess the probability of risk occurrence and its potential impact on the project using qualitative or quantitative methods.
   * Represent risks using a risk matrix (Probability vs. Impact).
3. **Risk Mitigation**
   * Develop strategies to minimize the likelihood of risks or reduce their impact.
   * Examples: Contingency planning, use of proven technologies, or resource reallocation.
4. **Risk Monitoring**
   * Continuously monitor identified risks and detect new risks throughout the project lifecycle.
   * Update the RMMM plan as required based on project progress.

**Benefits of RMMM Plan:**

* Reduces project delays and cost overruns.
* Enhances project stability and success.
* Improves team preparedness for unforeseen challenges.

### **Learning Objective:**

* To understand the principles of risk management in software projects.
* To identify, assess, mitigate, and monitor risks effectively.
* To develop a systematic approach to managing project risks.

### **Learning Outcome:**

At the end of this experiment, students will be able to:

1. Identify potential risks in their software project.
2. Formulate a detailed RMMM plan to manage risks.
3. Monitor risks and update the plan to ensure project stability.

### **Course Outcomes (COs):**

* **CO5:** Evaluate and mitigate software project risks and apply configuration management practices to maintain project integrity.

### **Cognitive Levels of Attainment as per Bloom’s Taxonomy:**

* **L3 (Apply):** Apply risk management principles to identify and mitigate project risks.
* **L5 (Evaluate):** Evaluate the effectiveness of the RMMM plan and suggest improvements.

### **Programme Outcome (POs):**

* **PO2: Problem Analysis:** Identify and analyze risks related to project requirements and constraints.
* **PO3: Design/Development of Solutions:** Design strategies to mitigate risks in software projects.
* **PO5: Engineering Tool Usage:** Utilize tools to monitor and document risks effectively.
* **PO10: Project Management and Finance:** Apply risk management principles to optimize project outcomes.

### **Programme Specific Outcome (PSO):**

* **PSO1:** Apply the culture of augmenting existing technologies to create sustainable IT solutions.
* **PSO2:** Integrate various technologies to address and mitigate risks in real-time project scenarios.

### **Result & Discussion:**

* **Result:** A detailed RMMM plan for the software project has been developed.
* **Discussion:**
  + Identified risks were categorized based on probability and impact.
  + Mitigation strategies were proposed and documented to address the top-priority risks.
  + The monitoring framework was established for continuous risk evaluation.

### **Conclusion:**

Developing an RMMM plan is crucial for ensuring project success. By completing this experiment, students gained hands-on experience in risk management, enhancing their ability to predict and manage challenges effectively in software engineering projects.

### **Steps for the Experiment**

#### ****1. Identify Project Risks****

1. Analyze the project scope, requirements, and resources to identify potential risks.
2. Classify risks into categories such as technical, resource, schedule, and operational risks.

#### ****2. Assess Risks****

1. Assign a probability (Low, Medium, High) and impact (Low, Medium, High) to each risk.
2. Create a risk matrix to prioritize risks based on their probability and impact.

#### ****3. Develop Mitigation Strategies****

1. For high-priority risks, propose actionable strategies to reduce probability or impact.
2. Document fallback plans for risks that cannot be mitigated entirely.

#### ****4. Establish Monitoring Framework****

1. Define metrics and tools for monitoring risks throughout the project lifecycle.
2. Assign responsibilities for risk tracking and reporting.

#### ****5. Prepare the RMMM Plan****

1. Compile all risk-related information into a structured RMMM document.
2. Include risk descriptions, assessment data, mitigation strategies, and monitoring plans.

### **Tools for Risk Management:**

* Risk Matrix Templates
* MS Excel or Google Sheets for tracking risks
* Project Management Tools (e.g., Jira, Trello)

### **Expense Splitter App (ESA)**

An **Expense Splitter App** allows users to share expenses efficiently among a group. It includes modules like expense entry, group management, payment tracking, and data visualization. Developing an RMMM plan for this system involves considering risks in areas such as:

* Technical Risks: Calculation errors, data storage issues, cross-browser compatibility problems.
* Operational Risks: Users forgetting to settle balances, duplicate expense entries, poor UI leading to confusion.
* Management Risks: Tight deadlines causing incomplete testing, scope creep due to last-minute feature requests.

**Procedure:**

**Risk Identification:**

* Conduct brainstorming sessions with the development team to identify potential risks.
* Review project documents such as requirements, UI/UX flows, and backend architecture to foresee possible risk areas.

Example Risks for ESA:

* Incorrect calculations leading to unfair expense distribution.
* Data loss due to local storage failure.
* Multiple users entering the same expense, causing duplicates.

**Risk Analysis:**

For each identified risk, assess its likelihood (high, medium, low) and its potential impact (severe, moderate, minor).

Example Analysis for ESA:

* Inaccurate calculations: Likelihood = High, Impact = Severe.
* Database loss: Likelihood = High, Impact = High.
* Duplicate expense entries: Likelihood = Medium, Impact = Moderate.

**Risk Mitigation:**

For each risk, develop strategies to reduce its impact or likelihood.

Example Mitigation Strategies for ESA:

* Incorrect calculations: Implement automated test cases for calculations.
* Data loss: Store data in IndexedDB and allow backup/export options.
* Duplicate entries: Implement a transaction confirmation mechanism.

**Risk Monitoring:**

* Set up error logging for critical functions (calculation, storage).
* Conduct weekly tests for expense tracking accuracy.
* Track risks in an issue management tool like Trello or Jira.

**Risk Management:**

* Continuously update the RMMM plan as new risks emerge.
* Assign owners for each risk and ensure mitigation actions are executed.

### **RMMM Plan:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Probability** | **Impact** | **Mitigation Strategy** | **Monitoring Plan** |
| R1 | Incorrect calculations in expense splitting | High | Severe | Implement unit tests for calculation functions. | Weekly testing and validation logs. |
| R2 | Data loss due to local storage issues | High | High | Store data in IndexedDB and allow backup/export options. | Check storage integrity every deployment. |
| R3 | Duplicate expense entries by multiple users | Medium | Moderate | Implement a confirmation prompt before adding an expense. | Track duplicate entries in error logs. |
| R4 | Users forgetting to settle expenses | High | Medium | Implement automatic reminders and notifications. | Check settlement status weekly. |
| R5 | Cross-browser compatibility issues | Medium | Medium | Test UI/UX on multiple browsers before deployment. | Conduct pre-release browser testing. |
| R6 | Tight deadlines leading to incomplete testing | High | High | Prioritize core features, then focus on enhancements. | Conduct weekly project progress reviews. |
| R7 | Unauthorized access to stored expense data | Medium | High | Implement authentication (PIN/password). | Monitor unauthorized access logs. |