**Name: Patel Muskan**

**Roll No: 22DCO04** **Batch:** 1 **Subject:** SE

# Experiment No. 11

**Aim:** Preparation of Risk Mitigation, Monitoring and Management Plan (RMMM).

# Theory:

Most software engineering projects are risky because of the range of serious potential problems that can arise. The primary benefit of risk management is to contain and mitigate threats to project success. You must identify and plan, and then be ready to act when a risk arises drawing upon the experience and knowledge of the entire team to minimize the impact to the project. Software Risk management includes the identification and classification of technical, programmatic and process risks, which become part of a plan that links each to a mitigation strategy. The project manager monitors risk during the project. If any materialize, a specific owner implements a mitigating action. In this article, we explain the elements of an effective software risk management plan and provide examples of plan elements. Software Risk Management Plan: - After cataloguing risks according to type (technical, project, process, organizational), the software development project manager crafts a plan to record and monitor these risks. As part of a larger, comprehensive project plan, the risk management plan outlines the response that will be taken for each risk- if it materializes. A comprehensive risk register would contain consist of the following attributes:

* Description of risk -Summary description of the risk- easy to understand.
* Recognition Date – Date on which stakeholders identify and acknowledge the risk.
* Probability of occurrence – Estimate of probability that this risk will materialize (%).
* Severity – The intensity of undesirable impact to the project – if the risk materializes.
* Owner- This person monitors the risk and acts if necessary
* Action – The contingent response if the risk materializes.
* Status – current team view of the risk potential, monitoring, occurring, or eliminated.
* Loss Size – Given in hours or days, this is a measure of the negative impact to the project.
* Risk Exposure – Given in hours or days, this is is a product of probability and loss size.
* Priority (optional) – This is either an independent ranking or the product of probability and severity. Typically, higher severity-risk with high probability has higher priority.

# Effective Strategies must consider three issues:

* Risk Avoidance.
* Risk Monitoring.
* Risk Management and contingency planning: Proactive approach to risk- avoidance strategy. Develop a strategy to mitigate the risk for reducing turnover.
* Meet the current staff to determine causes for turnover.
* Organize project teams so that information about each development activity is widely dispersed.
* Define documentation standards and establish mechanisms to be sure, that documents are developed in a timely manner. Project manager monitors for likelihood of risk. Project manager should monitor the effectiveness of risk mitigation steps. Risk management and contingency planning assumes that mitigation efforts have failed and that the risk has become a reality. RMMM steps in to cut additional project costs.

# The RMMM Plan:

Risk Mitigation, Monitoring and Management Plan - documents allwork performed as part of risk analysis and is used by the project manager as part of the overall project plan. RIS is maintained using a database system, so that creation and information entry, priority ordering, searches and other analysis may be accomplished easily. Risk monitoring isa project tracking activity.

# Primary Objectives:

* Assess whether predicted risks do, in fact, occur.
* Ensure that risk aversion steps defined for the risk are being properly applied.
* Collect information that can be used for future risk analysis.

# Risk Refinement:

At various points in the checklist, lack of software tools is identified as a potential risk. Due to time constraints, the members of the design team felt that searching for and learning to use additional software tools could be detrimental to the project, as it would take time away from project development. For this reason, we have decided to forgo the use of software tools. It will not be explored asa potential risk because al planning will be done without considering

their use.

# Risk Mitigation, Monitoring & Management:

* **Risk: Computer Crash**

# Mitigation:

The cost associated with a computer crash resulting in loss of data is crucial. A computer crash is not itself not crucial, but rather the loss of data. Also, the data will result in not being able to deliver the product to the customer. This will result in not receiving a letter and acceptance from the customer. Without the letter of acceptance. The group will receive a failing grade for the course. As a result, the organization is taking steps to make multiple backup copies of the software in development and all documentation associated with it, in multiple locations.

# Monitoring:

When working on the productor documentation, the staff members should always be aware of the stability of the computing environment they are working in. Any changes in the stability of the environment should be recognized and taken seriously.

# Management:

The lack of a stable-computing environment is extremely hazardous to a software development team.

# Risk: Technology Does Not Met Specifications

* + **Mitigation:**

To prevent this from happening, meetings will be held with the customer on a routine business. This ensures that the product we are producing, and the specifications of the customer are equivalent.

# Monitoring:

The meetings with the customer should ensure that the customer and out organization understand each other and the requirements for the project.

# Management:

The development team should come to the realization that their idea of the product specifications differs from those of the customer, the customer should be immediately notified and whatever steps necessary to rectify this problem should be done.

# Risk: End Users Resist System

* + **Mitigation:**

To Prevent this from happening software will be developed with the end user in mind. The user interface will be designed in a way to make sure use of the program is convenient and pleasurable.

# Monitoring:

The software will be developed with het end user in mind. The developmental team will ask the opinion of the various outside sources throughout het development phases. Specifically, the user-interface developer will be sure to get a thorough opinion from others.

# Management:

The program should be resisted by the ned user, the program will be thoroughly examined to find t h e reasons that this is so. Specifically, the user interface will be investigated and if necessary, revamped into a solution.

**Risk Probability Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risks** | **Category** | **Probability** | **Impact** |
| Equipment Failure | TI | 70% | 1 |
| Technology will not meet expectations | TE | 30% | 1 |
| End users resist system | BU | 25% | 1 |
| Changes in  requirements | PS | 20% | 2 |
| Deviation from software engineering  standards | PI | 10% | 3 |
| Less reuse than planned | PS | 50% | 3 |
| Poor comments in code | TI | 25% | 4 |

**Implementation:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Information Sheet** | | | | |
| **Project Name: Edufund - Education Fundraising Website** | | | | |
| **Risk Id:** 001 | **Date:** 04/09/2023 | | **Probability:** 50% | **Impact:** Average |
| **Description:**  Our project, Edufund, faces several risks related to security, performance, user-friendliness, data accuracy, and integration with other systems. | | | | |
| **Refinement/Monitoring:**  Regular security updates and code reviews to protect user data.  Continuous monitoring and load testing to ensure optimal website performance.  Regular usability testing and gathering feedback to enhance the user experience.  Implementing robust data validation mechanisms for data accuracy.  Ensuring a clear understanding of integration points with other systems. | | | | |
| **Mitigation/ Monitoring:**  Implementing strong security measures, including penetration testing and staff training for data protection.  Conducting performance testing, optimizing the website, and fine-tuning for efficiency.  Actively involving users in usability testing to improve the website's user-friendliness.  Implementing data validation, encryption, and regular backups to safeguard critical information.  Conducting comprehensive integration testing and maintaining constant communication with third-party systems. | | | | |
| **Contingency Plan/Trigger:**  Launch of new features to enhance the platform's capabilities.  A significant increase in user activity or load on the website.  Gathering user feedback that indicates UI/UX improvements are necessary.  Instances of data input errors or unauthorized data access.  Changes in third-party systems, including version updates that may affect integration. | | | | |
| **Originator:** Prof. Abdul Majid Ansari | | **Assigned:** Team Tech Brains | | |

# Conclusion:

Thus, we have successfully studied the Preparation of Risk Mitigation, Monitoring and Management Plan (RMMM).