Experiment No. 9

Title: Preparation of RMMM Plan

Name of Student: Owais Mirajkar

Roll No. : 26

Date : ____ / ____ / ________

Subject In -charge Sign:

……………………………….

Experiment No. 9

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

Theory:

RMMM Plan:

A risk management technique is usually seen in the software Project plan. This can be divided into Risk Mitigation, Monitoring, and Management Plan (RMMM). In this plan, all works are done as part of risk analysis. As part of the overall project plan project manager generally uses this RMMM plan.

In some software teams, risk is documented with the help of a Risk Information Sheet (RIS). This RIS is controlled by using a database system for easier management of information i.e creation, priority ordering, searching, and other analysis. After documentation of RMMM and start of a project, risk mitigation and monitoring steps will start.

Risk Mitigation :

It is an activity used to avoid problems (Risk Avoidance).

Steps for mitigating the risks as follows.

1. Finding out the risk.
2. Removing causes that are the reason for risk creation.
3. Controlling the corresponding documents from time to time.
4. Conducting timely reviews to speed up the work.

Risk Monitoring :

It is an activity used for project tracking.

It has the following primary objectives as follows.

1. To check if predicted risks occur or not.
2. To ensure proper application of risk aversion steps defined for risk.
3. To collect data for future risk analysis.
4. To allocate what problems are caused by which risks throughout the project.

Risk Management for User Authentication System

Two-factor authentication, which uses two of the above mentioned combined.

Multi-factor authentication, which uses all three ways of authentication; such as your user name and password, combined with a text code sent to your cell phone and your fingerprint.

Single sign-on (SSO) coordinates login to multiple applications with a single, strong authentication.

Centralized authentication, which is a lot like SSO, but requires a user who has logged into the first application to re-enter the password even though the credentials are the same.

Risk Mitigation

Develop a strong password policy:-
Establish clear password requirements, such as the use of uppercase and lowercase letters combined with numbers or special characters.

Crack down on password sharing and the sharing of user accounts.

Require unique passwords and pass phrases for each user.

Centralized authentication mitigation:-

Centralized authentication mitigates password management risk by consolidating login information shared across multiple applications. Unlike SSO, centralized authentication requires constant repetition of credentials.

With centralized authentication, employees have a single username and password that works across multiple applications. This means that, similar to SSO, they need to remember only a single password.

With centralized authentication, however, they need to enter those credentials every time they open a new application.

Two-factor authentication:-
Two-factor authentication is rapidly becoming a necessary and common safety protocol. It requires a username and password, and a piece of additional information tied to either an object or their person.

Biometric authentication takes password management risk mitigation to the next level by requiring the use of information specific to the individual person, not just to something he or she owns. This can involve facial, fingerprint, or voice recognition.

Risk Management and planning:

It assumes that the mitigation activity failed and the risk is a reality. This task is done by Project manager when risk becomes reality and causes severe problems. If the project manager effectively uses project mitigation to remove risks successfully then it is easier to manage the risks. This shows that the response that will be taken for each risk by a manager. The main objective of the risk management plan is the risk register. This risk register describes and focuses on the predicted threats to a software project.

Conclusion: After successful completion of this lab, the student will have the ability to identify risks, monitoring the risks and managing of those risks.