SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

# Software Engineering - Experiment 8

SAP ID: **60004210155, 60004210166, 60004220130**
Name: **Jigar Siddhpura, Aman Nambisan, Falguni Parmar**
Div: **C2**
Batch: **C22**

**Aim:** Create a Risk Mitigation, Monitoring and Management Plan

**Theory:** RMMM, also known as Risk Mitigation, Monitoring, and Management, is a framework or methodology used to effectively identify, assess, and address risks in a systematic manner throughout the lifecycle of a project or system. It provides a structured approach for managing risks to minimize their potential negative impact and ensure the successful completion of a project. Here's a theoretical overview of the RMMM framework:

- Risk Identification: The first step in the RMMM process is to identify potential risks that could impact the project or system. This involves systematically examining various aspects, such as technology, resources, stakeholders, requirements, and external factors, to identify potential risks and their sources.

- Risk Assessment: Once risks are identified, they need to be assessed to understand their likelihood of occurrence and potential impact on the project. This involves evaluating the probability, severity, and detectability of each risk to prioritize them based on their significance.

- Risk Mitigation: Risk mitigation involves developing strategies and actions to reduce the probability or impact of identified risks. This could include implementing preventive measures, such as improving security controls, conducting thorough testing, or implementing redundancy. The goal is to minimize the likelihood or severity of risks and enhance the project's resilience.

- Risk Monitoring: Throughout the project lifecycle, risks need to be continuously monitored to detect any changes or new risks that may arise. This involves tracking and analyzing risk indicators, metrics, and triggers to identify warning signs or deviations from expected outcomes. Regular monitoring enables proactive risk management and timely intervention.

- Risk Management: Risk management is an ongoing process that involves decision-making, planning, and coordination to address risks effectively. This includes assigning responsibilities, establishing communication channels, and

defining escalation procedures to ensure that risks are managed and mitigated in a coordinated and timely manner.

- Documentation and Lessons Learned: It is essential to document all identified risks, their assessment, mitigation strategies, and the outcomes of risk management activities. This documentation serves as a valuable reference for future projects and enables the organization to learn from past experiences, continuously improve risk management practices, and apply lessons learned.

By following the RMMM framework, organizations can systematically address risks throughout the project lifecycle, enhance decision-making, and improve overall project success rates. It provides a structured approach to identify, assess, mitigate, and monitor risks, enabling stakeholders to have better visibility and control over potential threats and uncertainties.

**Risk Table:**

| Risks | Category | Probability | Impact |
|---|---|---|---|
| Equipment failure | TI | 70% | 1 |
| Late delivery | BU | 30% | 1 |
| Technology will not meet expectations | TE | 25% | 1 |
| End users resist system | BU | 20% | 1 |
| Changes in requirements | PS | 20% | 2 |
| Fluctuations in cryptocurrency prices | BU | 50% | 2 |
| Regulatory changes in Cryptocurrency | PS | 15% | 3 |
| Less reuse than planned | PS | 60% | 3 |
| Payment disputes | BU | 30% | 3 |

| | | | |
|---|---|---|---|
| Smart contract vulnerabilities | TE | 25% | 4 |



| | | | |
|---|---|---|---|
| Poor comments in code | TI | 20% | 4 |
| Cybersecurity breaches | TI | 40% | 4 |

## Risk Information Sheet (RIS) for risk no. 10 :

| Risk Information Sheet | | |
|---|---|---|
| **Risk ID** : P02-4-32 | **Date** : 3/4/24 | **Prob** : 25% |
| **Description :** Smart contracts are self-executing computer programs that are stored on a blockchain. They can be used to automate processes , create decentralized applications, and facilitate transactions. However, smart contracts are also vulnerable to security risks including coding erros, design flaws, and other vulnerabilities that could lead to exploitation and financial losses. | | |
| **Refinement /Context**<br>Subcondition 1- The smart contract code is not thoroughly reviewed before deployment.<br>Subcondition 2- The smart contract is not tested under different conditions before deployment.<br>Subcondition 3- The smart contract is not audited by an external security team.<br>Subcondition 4- The smart contract is not updated regularly to address newly discovered vulnerabilities.<br>Subcondition 5- The smart contract is not deployed on a secure and reliable blockchain platform.<br>Subcondition 6- The deployment team lacks knowledge and experience in smart contract security. | | |
| **Mitigation /Monitoring:**<br>1. Use of well-tested and audited smart contract libraries and frameworks.<br>2. Ensure secure coding practices, such as input validation and proper error handling, and followed during smart contract development.<br>3. Conduct regular security assessments and penetration testing to identify and mitigate vulnerabilities.<br>4. Implement a bug bounty program to incentivize researchers to identify and report vulnerabilities.<br>5. Monitor the blockchain network and smart contracts for suspicious activity using blockchain monitoring tools.<br>6. Have a disaster recovery plan in place to address security incidents and minimize impact.<br>7. Stay up to date on the latest security threats and developments in the blockchain and smart contract space. | | |
| **Management /Contingency Plan /Trigger:**<br>Allocate budget for regular security audits and penetration testing of smart contracts.<br>Ensure smart contract developers undergo thorough security training.<br>Develop a contingency plan for response to security breaches or incidents involving smart contracts.<br>**Trigger**: security breaches or incidents involving smart contracts | | |
| **Current Status** :<br>No significant smart contract vulnerabilities have been identified in the system as of the last security audit conducted on April 3, 2024.<br>However, continuous monitoring and testing are being carried out to ensure the system remains secure against potential vulnerabilities | | |
| **Originator** : Jigar Siddhpura | **Assigned** : Aman Nambisan | |