NAME:	Deepanshu Aggarwal, Kunal Bhatia
UID:	2021300002, 2021300010
SUBJECT	SE
EXPERIMENT NO :	8
AIM:	Develop Risk Mitigation, Monitoring and Management Plan for the case study.
THEORY	**RMMM Plan for Crime Reporting System Project:** **Risk Mitigation:** 1. Identifying Risks: - Conduct a thorough analysis to identify potential risks related to cybersecurity, user adoption, legal compliance, and system performance. 2. Addressing Causes: - Invest in state-of-the-art cybersecurity measures to prevent unauthorized access and data breaches. - Implement user-friendly features to enhance user adoption and satisfaction. - Conduct regular legal reviews to ensure compliance with data protection and privacy laws. - Perform system performance testing to identify and address potential bottlenecks. 3. Document Control: - Establish a system to control and update relevant documents regularly, including privacy policies, user guides, and compliance documentation. 4. Timely Reviews: - Conduct regular reviews of the Crime Reporting System to identify areas for improvement in terms of user experience, legal compliance, and system performance. **Risk Monitoring:** 1. Checking Predicted Risks: - Continuously monitor potential risks related to cybersecurity, user adoption, legal compliance, and system performance.

2. Applying Risk Aversion Steps:
- Ensure that the risk mitigation steps outlined in the plan are consistently applied, focusing on cybersecurity measures, user engagement, and legal compliance.

3. Data Collection:
- Collect data on user interactions, system performance, and any security incidents for future analysis and improvement of the Crime Reporting System.

4. Problem Allocation:
- Attribute issues that arise during the project to specific risks, aiding in understanding the effectiveness of risk mitigation strategies.

Risk Management and Planning:

1. Assuming Risk Reality:
- Assume that despite mitigation efforts, certain risks may become a reality. Develop contingency plans for each identified risk scenario, including legal challenges or system performance issues.

2. Response Planning:
- Clearly define response actions for each risk, specifying roles and responsibilities in the event of a risk becoming a reality. This includes legal responses, public relations strategies, and technical solutions.

3. Risk Register:
- Maintain a comprehensive risk register that focuses on predicted threats to the Crime Reporting System project, including details on mitigation strategies and contingency plans.

Example - User Adoption Challenge:

Risk Mitigation:
- Implement user-centric design principles to enhance the user experience.
- Conduct user testing and feedback sessions during the development phase.
- Develop a robust marketing and awareness campaign to promote the Crime Reporting System among the target audience.

Risk Monitoring:
- Monitor user engagement metrics, such as the number of reports filed and user feedback.

	- Collect and analyse user feedback regularly to identify areas for improvement. Risk Management: - If user adoption is lower than expected, initiate targeted marketing efforts to increase awareness. - Collaborate with marketing experts to refine promotional strategies and improve user engagement. **Additional Risk Scenarios:** **CR5: Insufficient Data Encryption** Mitigation: - Implement end-to-end encryption for all user data. - Regularly update encryption protocols to stay ahead of potential vulnerabilities. Monitoring: - Conduct regular security audits to ensure the effectiveness of encryption measures. Management: - In case of a breach, activate the incident response plan, including notifying affected users and authorities. **CR6: Inadequate Legal Compliance** Mitigation: - Regularly review and update privacy policies and terms of service. - Consult legal experts to ensure compliance with evolving data protection laws. Monitoring: - Stay informed about changes in data protection regulations and adjust policies accordingly. Management: - In case of legal challenges, collaborate with legal experts to address issues promptly. Drawbacks of RMMM for Crime Reporting System Project: - Increased project costs.

	- Additional time requirements. - Implementation of RMMM may become a complex project, especially for larger projects. - RMMM does not guarantee a risk-free project; unforeseen risks may still emerge even after the website's launch.

Risk Assessment Table:

RID	Risk Description	Impact	Probability of loss	Size of loss(in days)	Risk Exposure(days)
CR1	Unauthorized access to sensitive user information	3	40%	7	2.8
CR2	Legal challenges due to non-compliance	2	30%	5	1.5
CR3	System vulnerabilities exploited by hackers	4	25%	10	2.5
CR4	Poor user adoption of the Crime Reporting System	3	20%	6	1.2
CR5	Insufficient data encryption	3	25%	8	2.0
CR6	Inadequate legal compliance	2	20%	4	0.8

Impact values:
1-Catastrophic
2-Critical
3-Marginal
4-Negligible
Risk Exposure = Probability of loss * Size of loss

RMMM Plan:

Risk Information Sheet		
Risk ID: **CR1**	11-01-2023	40%
Description: The risk involves the possibility of unauthorized access to sensitive user information.		
Mitigation/Monitoring: -Implement robust user authentication mechanisms, such as multi-factor authentication. -Encrypt sensitive user data both in transit and at rest. -Regularly update access control policies based on the principle of least privilege. -Conduct regular penetration testing to identify and rectify vulnerabilities.		

Management/Contingency Plan/Trigger: -In case of a security breach, activate the incident response plan. -Notify affected users and relevant authorities promptly. -Collaborate with cybersecurity experts to assess the extent of the breach and implement additional security measures.
Current Status: 11-01-2023: Mitigation steps underway.

Risk Information Sheet		
Risk ID: CR2	11-01-2023	30%
Risk Description: The risk involves legal challenges due to non-compliance with data protection and privacy laws.		
Mitigation/Monitoring: -Regularly review and update privacy policies and terms of service. -Conduct legal compliance audits to ensure adherence to evolving data protection regulations. -Collaborate with legal experts to stay informed about changes in relevant laws. **Management/Contingency Plan/Trigger:** -In case of legal challenges, activate the legal response plan. -Collaborate with legal experts to address issues promptly. -Update policies and practices based on legal recommendations.		
Management/Contingency Plan/Trigger: 1. In case of a breach, activate the incident response plan, including notifying affected users and authorities. 2. Collaborate with cybersecurity experts to address the breach and implement additional security measures.		
Current Status: 11-01-2023: Mitigation steps underway.		

Risk Information Sheet		
Risk ID: CR3	11-01-2023	25%
Risk Description: The risk involves the possibility of system vulnerabilities being exploited by hackers.		
Mitigation/Monitoring: -Implement regular security audits and updates to address potential vulnerabilities. -Collaborate with cybersecurity experts for penetration testing to identify and fix weaknesses. -Stay informed about the latest cybersecurity threats to adjust security measures accordingly.		
Management/Contingency Plan/Trigger: 1. In case of a breach, activate the incident response plan, including notifying affected users and authorities. 2. Collaborate with cybersecurity experts to address the breach and implement additional security measures.		
Current Status: 11-01-2023: Mitigation steps underway.		

Risk Information Sheet		
Risk ID: CR4	11-01-2023	20%
Risk Description: The risk involves poor user adoption of the Crime Reporting System		
Mitigation/Monitoring: -Implement user-centric design principles to enhance the user experience. -Conduct user testing and feedback sessions during the development phase. -Develop a robust marketing and awareness campaign to promote the Crime Reporting System among the target audience.		
Management/Contingency Plan/Trigger: 1. In case of a breach, activate the incident response plan, including notifying affected users and authorities. 2. Collaborate with cybersecurity experts to address the breach and implement additional security measures.		
Current Status: 11-01-2023: Mitigation steps underway.		

Risk Information Sheet		
Risk ID: CR5	10-01-2023	25%
Risk Description: The risk involves the possibility of insufficient data encryption, leading to potential breaches.		
Mitigation/Monitoring: 1. Implement end-to-end encryption for all user data. 2. Regularly update encryption protocols to stay ahead of potential vulnerabilities. 3. Conduct regular security audits to ensure the effectiveness of encryption measures.		
Management/Contingency Plan/Trigger: 1. In case of a breach, activate the incident response plan, including notifying affected users and authorities. 2. Collaborate with cybersecurity experts to address the breach and implement additional security measures.		
Current Status: 11-01-2023: Mitigation steps underway.		

Conclusion:

From this adaptation, it's evident that assessing risks, tabulating them for analysis, and developing strategies for mitigation and management are crucial for the successful implementation of a Crime Reporting System. Regular monitoring and adjustments based on evolving threats contribute to the long-term success and security of the project.