Name: Prerna Sunil Jadhav
Sap Id: 60004220127
Course: Software Engineering
Course code: DJ19CEC601
Branch: Computer Engineering
Batch: C2-2

EXPERIMENT 08

AIM: To create a RMMM plan. Create risk assessment technique template for a case study.

THEORY:

#RISKS FOR LAWYER MANAGEMENT SYSTEM.

1) Inadequate Requirements Gathering (R001):
Risk of not fully understanding client needs & system requirements during the initial phase of development.

2) Technical complexity (R002):
Complexity of integrating various modules & functionalities within the system, leading to potential delays or errors in development

3) Resource constraints (R003):
Insufficient availability of skilled developers or resources to meet project deadlines

4) Security Vulnerabilities (R004):
Risk of data breaches or unauthorized access to sensitive legal information within system

5) Integration Challenges:
Difficulties in integrating third-party systems or components with LMS, leading to interoperability issues

6) Scope Creep:
Continuous expansion of project scope beyond initial requirement, leading to schedule & budget overrun

7) Dependency Risks:
PRoject dependencies on external factors such as third party APIs, services which may impact project

8) Lack of stakeholders Engagement:
Insufficient involvement or feedback leads to misalignment

9) Data Integrity Risks:
Risks associated with inaccurate or incomplete data within system, leading to error or inconsistencies in legal proceedings or client information.

10) Regulatory compliance Risks:
failure to comply with legal & regulatory requirements governing the management & storage of legal documents & client information

Risk Table:

TI: Technical Issue	CR: Customer Related Risks
TR: Technical Risks	BU: Business Impact Risks
PR: Process Risks	

Critical: 2
Medium: 1
Low: 0

RISK	category	Probability	Impact
1) Inadequate Requirement gathering	PR	30	2
2) Technical complexity	TI	25	2
3) Resource constraints	BU	20	1
4) security Vulnerabilities	TR	40	2
5) Integration Challenges	TI	35	2
6) Scope Creep	PR	25	1
7) Dependency Risks	BU	30	2
8) Lack of Stakholder Engagement	CR	20	1
9) Data Integrity Risks	TR	35	2
10) Regulatory compliance Risks	BU	30	2

Let the cutoff be probability 30% & impact being 2, so for RIS we choose security vulnerabilities and make RIS for that Risk

CONCLUSION: Hence, we understood what RMMM plan is & how to make it & made one for our case study.
Also we identified 10 Risks and understanding this risks, so can mitigate potential challenges.

Name (Sap Id):	Kalpita Shankhdhar (60004210164) Akshata Sunil Dharmadhikari (60004220125) Prerna Sunil Jadhav (60004220127)
Class:	T. Y. B. Tech (Computer Engineering)
Course:	Software Engineering Laboratory
Course Code:	DJ19CEL601
Experiment No.:	08

RISK INFORMATION SHEET

RISK INFORMATION SHEET			
RISK ID: R004	**Date: 25/04/2024**	**Prob: 20%**	**Impact: Critical (2)**
Description: Security vulnerabilities pose the risk of data breaches or unauthorized access to sensitive legal information within the system**.**			
Refinement/Context: **Sub Condition 1:** Insufficient encryption protocols in place for data storage and transmission. **Sub Condition 2:** Lack of regular security updates and patches for system components**.** **Sub Condition 3:** Weaknesses in authentication and authorization mechanisms**.**			
Mitigation/Monitoring: 1. Implement robust encryption algorithms for sensitive data both in transit and at rest. 2. Regularly update and patch system components to address known security vulnerabilities. **3.** Enhance authentication mechanisms with multi-factor authentication and role-based access control**.**			
Management/Contingency Planning/Trigger: 1. Detection of unauthorized access attempts or security breaches in system logs. **2.** Discovery of vulnerabilities during security audits or penetration testing.			
Current status: 27/04/2024: Mitigation steps initiated			
Originator: Akshata Dharmadhikari		**Assigned:** Prerna Jadhav, Kalpita Shankhdhar	