Software Risk Management Plan

College Complaint Management System

1. Introduction

This Software Risk Management Plan is prepared for the College Complaint Management System based on the given case study. The document follows the same structure and headings as the sample risk management document. The purpose of this plan is to identify, analyze, and manage potential risks that may arise during the development and deployment of the system.

2. Risk Identification

Risk identification involves recognizing possible risks that could affect the successful implementation of the College Complaint Management System. The identified risks include:

- Technical Risks – Server downtime, software bugs, database failures, or security vulnerabilities.
- Schedule Risks – Delays due to requirement changes or limited development time.
- Cost Risks – Budget overruns caused by additional infrastructure or maintenance needs.
- Resource Risks – Lack of skilled developers, administrators, or support staff.
- Operational Risks – Delayed complaint updates by departments or improper system usage.

3. Risk Analysis

Risk analysis evaluates the probability and impact of identified risks.

- Technical Risks – High impact, medium probability, as system failure directly affects users.
- Schedule Risks – Medium impact and probability due to academic deadlines.
- Cost Risks – Low to medium probability but moderate impact on project sustainability.
- Resource Risks – Medium probability and impact depending on staff availability.
- Operational Risks – High probability with medium impact if users do not follow procedures.

This analysis helps prioritize risks and allocate appropriate mitigation strategies.

4. Risk Mitigation

Risk mitigation strategies are defined to reduce or eliminate identified risks:

- Implement regular system testing and code reviews to minimize technical risks.
- Maintain a realistic project schedule with buffer time.
- Allocate contingency funds to manage unexpected costs.
- Provide training to developers, administrators, and department staff.

• Establish clear operational guidelines and monitoring mechanisms.

These strategies help ensure smooth system development and operation.

5. Risk Monitoring

Risk monitoring is a continuous process throughout the project lifecycle. Regular reviews are conducted to track identified risks and detect new ones. System performance, security logs, and user feedback are monitored to ensure timely corrective actions. Proper documentation and reporting help maintain effective risk control.