# RISK ASSESSMENT SHEET

**Project:** Lecture Scheduling System  
**Version:** 1.0  
**Date:** 2025-10-07  
**Prepared By:** Timetable Buddy Engineering Team

|  |  |
| --- | --- |
| Name | Roll Number |
| Sarthak Kulkarni | 23101B0019 |
| Dhruv Tikhande | 23101B0005 |
| Atharv Petkar | 23101B0010 |
| Pulkit Saini | 23101B0021 |

## Document Overview

This document contains a comprehensive risk assessment for the Lecture Scheduling System software development project. Each risk is analyzed for probability (shown as percentage) and impact, with detailed mitigation, monitoring, and management plans.

### Risk Assessment Criteria:

**Impact Levels:**

* **Critical:** Severe impact on project success, may cause project failure
* **High:** Significant impact on schedule, budget, or quality
* **Medium:** Moderate impact, manageable with effort
* **Low:** Minor impact, easily resolved

## Risk Assessment Details

### Risk #1

| **Risk ID** | **R-TTB-005** | **Type** | **Technical** |
| --- | --- | --- | --- |
| Probability | 10% | Impact | Critical |
| Risk Description | Critical security vulnerability discovered in production system allowing unauthorized data access. |  |  |
| Mitigation plan | 1. Conduct regular security audits and penetration testing. 2. Implement security scanning in CI/CD. 3. Follow OWASP guidelines. |  |  |
| Monitoring plan | Run automated security scans weekly. Monitor security patch releases for dependencies. |  |  |
| Management plan | Deploy emergency patch within 4 hours. Notify affected users. Conduct incident post-mortem. |  |  |

### Risk #2

| **Risk ID** | **R-TTB-008** | **Type** | **Technical** |
| --- | --- | --- | --- |
| Probability | 15% | Impact | High |
| Risk Description | Cloud service provider experiences prolonged outage affecting application availability. |  |  |
| Mitigation plan | 1. Implement multi-region deployment. 2. Design for high availability. 3. Have disaster recovery plan. |  |  |
| Monitoring plan | Subscribe to cloud provider status updates. Monitor service health across regions. |  |  |
| Management plan | Failover to backup region. Communicate status to users. Document incident for review. |  |  |

### Risk #3

| **Risk ID** | **R-TTB-015** | **Type** | **External** |
| --- | --- | --- | --- |
| Probability | 15% | Impact | High |
| Risk Description | Vendor lock-in prevents migration to alternative solutions, increasing long-term costs. |  |  |
| Mitigation plan | 1. Use open standards where possible. 2. Design abstraction layers for vendor services. 3. Evaluate vendor independence regularly. |  |  |
| Monitoring plan | Review vendor contracts annually. Assess switching costs and alternatives. |  |  |
| Management plan | Plan phased migration to alternative vendor. Negotiate better terms with current vendor. Implement vendor-agnostic architecture. |  |  |

### Risk #4

| **Risk ID** | **R-TTB-018** | **Type** | **External** |
| --- | --- | --- | --- |
| Probability | 12% | Impact | Critical |
| Risk Description | Competitor launches similar product first, reducing market opportunity. |  |  |
| Mitigation plan | 1. Conduct competitive analysis regularly. 2. Focus on unique value propositions. 3. Plan for rapid iteration. |  |  |
| Monitoring plan | Monitor competitor activities and product launches. Track market trends and customer feedback. |  |  |
| Management plan | Accelerate development of differentiating features. Adjust marketing strategy. Consider strategic partnerships. |  |  |

### Risk #5

| **Risk ID** | **R-TTB-024** | **Type** | **Operational** |
| --- | --- | --- | --- |
| Probability | 15% | Impact | High |
| Risk Description | Inadequate disaster recovery procedures lead to extended downtime after incident. |  |  |
| Mitigation plan | 1. Document and test DR procedures quarterly. 2. Automate recovery processes. 3. Maintain offsite backups. |  |  |
| Monitoring plan | Test disaster recovery plan every 6 months. Track RTO and RPO metrics. |  |  |
| Management plan | Execute disaster recovery plan. Communicate with stakeholders. Document incident for improvement. |  |  |

## Risk Summary

**Total Risks Included:** 5  
**Criteria:** Only risks with probability ≤15%

### Risks by Impact:

* **Critical Impact:** 2 risk(s)
* **High Impact:** 3 risk(s)

## Risk Management Process

### 1. Risk Identification

* Conduct risk identification workshops at project initiation and quarterly
* Encourage all team members to report potential risks
* Review lessons learned from previous projects

### 2. Risk Assessment

* Evaluate each risk for probability (as percentage) and impact
* Calculate risk score (Probability × Impact)
* Prioritize risks based on score

### 3. Risk Mitigation

* Develop proactive plans to reduce probability or impact
* Assign risk owners for each identified risk
* Implement mitigation strategies before risks materialize

### 4. Risk Monitoring

* Track identified risks throughout project lifecycle
* Update risk status in weekly project meetings
* Use risk dashboard for visibility

### 5. Risk Management

* Execute management plans when risks occur
* Document lessons learned
* Update risk assessment based on new information

## Review and Updates

This risk assessment should be:

* **Reviewed:** Weekly in project status meetings
* **Updated:** When new risks are identified or risk status changes
* **Revised:** Monthly to reflect current project conditions
* **Archived:** At project completion for future reference

## Escalation Criteria

Risks should be escalated to senior management when:

* Impact level is Critical
* Mitigation plans are not effective
* Additional resources or authority needed

**Document Version:** 1.0  
**Last Updated:** 2025-10-07  
**Next Review Date:** 2025-10-14

**END OF DOCUMENT**