RMMM Table for SQA BankPro Project

This Risk Management, Mitigation, and Monitoring (RMMM) table outlines the key risks identified in the SQA BankPro project, along with their probability, impact, mitigation strategies, and monitoring approaches. Effective management of these risks ensures the successful development and deployment of the system.

| **Risk ID** | **Risk Description** | **Probability** | **Impact** | **Mitigation Strategy** | **Monitoring & Management** |
| --- | --- | --- | --- | --- | --- |
| R1 | Technical Failure: Server crashes or downtime affecting user access | Medium | High | Use load balancers, deploy redundant servers, implement auto-scaling and backups | Monitor server health, uptime, and error logs continuously |
| R2 | Scope Creep: Additional features requested beyond initial plan | High | High | Define detailed project scope and use strict change management processes | Regular scope reviews and stakeholder sign-offs on changes |
| R3 | Data Loss or Breach: Loss of sensitive banking data or security breach | Low | High | Implement strong encryption, regular database backups, and strict access controls | Continuous security monitoring, audit trails, and regular penetration testing |
| R4 | Integration Delays: Delays connecting frontend with backend or third-party APIs | Medium | Medium | Plan integration milestones early, conduct interface testing, and buffer timeline | Track integration status and conduct end-to-end testing regularly |
| R5 | Communication Gaps: Misalignment between dev team, stakeholders, and QA | Medium | Medium | Maintain clear communication channels, frequent updates, and documentation | Hold regular meetings, gather feedback, and document decisions |
| R6 | Developer Turnover: Losing key MERN stack developers mid-project | Medium | High | Cross-train team, maintain good documentation, and incentivize retention | Monitor team health and knowledge sharing sessions |
| R7 | Regulatory Compliance: Ensuring app meets banking regulations and data privacy laws | Low | High | Keep updated with relevant regulations (e.g., PCI DSS, GDPR), conduct compliance reviews | Regular compliance audits and update policies as regulations evolve |