**Table of Contents**

1. Risk Identification
2. Risk Analysis
3. Mitigation Strategies
4. Contingency Plans
5. Monitoring & Reporting

**1. Risk Identification**

| **Risk ID** | **Risk Description** | **Category** |
| --- | --- | --- |
| R1 | Delay in design approval | Schedule |
| R2 | Security vulnerabilities | Technical/Security |
| R3 | Third-party integration failures | Integration |
| R4 | Scope creep leading to budget overrun | Scope/Financial |
| R5 | Regulatory compliance issues | Compliance/Legal |

**2. Risk Analysis**

| **Risk ID** | **Likelihood** | **Impact** | **Priority** |
| --- | --- | --- | --- |
| R1 | Medium | High | 1 |
| R2 | Medium | Very High | 2 |
| R3 | Low | Medium | 3 |
| R4 | High | High | 1 |
| R5 | Low | High | 2 |

**3. Mitigation Strategies**

* **R1:**
  + Schedule buffer periods; arrange weekly design review meetings.
* **R2:**
  + Implement rigorous security testing and code reviews; engage third-party security experts.
* **R3:**
  + Initiate early testing with third-party vendors; maintain open communication channels.
* **R4:**
  + Enforce strict change control via Jira; conduct regular scope reviews.
* **R5:**
  + Consult legal/compliance teams throughout development.

**4. Contingency Plans**

* Develop alternative timelines and resource reallocation plans.
* Maintain backup vendors or technical resources for rapid intervention if necessary.

**5. Monitoring & Reporting**

* Track risks via a dedicated Jira board.
* Report risk status in weekly management meetings.
* Update risk assessments at major project milestones.