**Integrated Risk Management Plan**

**Project:** Odoo ERP Integration for Safaricom Telecom  
**Version:** 1.0  
**Date:** [Insert Date]

**A. Risk Management Objectives**

* Identify and assess risks early to minimize impact on project objectives.
* Implement effective mitigation and contingency plans.
* Assign clear ownership for risk monitoring and response.
* Ensure continuous risk communication and reporting.

**B. Risk Management Process**

| **Phase** | **Activity** | **Description** | **Responsibility** |
| --- | --- | --- | --- |
| Risk Identification | Workshops, Interviews, Document Reviews | Identify potential risks across scope, schedule, cost, quality, and compliance | Project Manager, Team Leads |
| Risk Assessment | Probability and Impact Analysis | Assess likelihood and impact; prioritize risks | Risk Owner, PMO |
| Risk Response Planning | Develop Mitigation and Contingency Plans | Define actions to reduce risk probability or impact and contingency steps if risk occurs | Risk Owner, Project Manager |
| Risk Monitoring & Control | Regular Reviews and Updates | Track risk status, effectiveness of responses, escalate as needed | PMO, Risk Owner |

**C. Risk Register (Sample Entries)**

| **Risk ID** | **Risk Description** | **Probability** | **Impact** | **Priority** | **Mitigation Strategy** | **Contingency Plan** | **Owner** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R1 | Delays in obtaining OSS/BSS integration specs | Medium | High | High | Engage OSS/BSS teams early; establish SLAs for information delivery | Allocate buffer time in schedule; escalate delays | Integration Lead |
| R2 | Data migration errors causing billing discrepancies | Medium | High | High | Conduct data profiling, cleansing, pilot migrations | Implement rollback plan; maintain legacy system fallback | Data Migration Lead |
| R3 | Resistance from users to new ERP processes | High | Medium | High | Develop comprehensive change management and training plans | Provide additional user support and coaching | Change Manager |
| R4 | Regulatory changes increasing project scope or requirements | Low | High | Medium | Monitor regulatory landscape continuously | Reassess scope and timeline; negotiate phased delivery | Compliance Officer |
| R5 | Vendor delays impacting custom development deliverables | Medium | Medium | Medium | Define clear SLAs; conduct vendor performance reviews | Activate backup vendor resources or internal staff | Vendor Manager |
| R6 | Security vulnerabilities at integration points | Medium | High | High | Perform security assessments and penetration tests | Apply patches and emergency fixes; conduct incident response | Security Officer |

**D. Risk Mitigation Strategies**

* **Early Stakeholder Engagement:** Build collaboration with all key stakeholders to identify and resolve potential blockers early.
* **Phased Implementation:** Use iterative rollouts to minimize impact of any one failure.
* **Robust Testing:** Extensive unit, integration, and UAT testing to uncover issues before production.
* **Comprehensive Training:** Prepare users to reduce resistance and errors.
* **Strict Change Control:** Manage scope creep and unexpected requirements carefully.

**E. Contingency Strategies**

* **Fallback Plans:** Maintain legacy systems operational during transition.
* **Schedule Buffers:** Include time reserves for high-risk activities.
* **Alternate Vendors:** Pre-qualify secondary vendors for critical deliverables.
* **Incident Response:** Develop plans for data breaches or system outages.
* **Escalation Procedures:** Clear pathways for escalating risks to executive sponsors.

**F. Risk Communication**

* Regular risk status updates in weekly project meetings.
* Risk dashboards accessible to all governance levels.
* Immediate notification for critical or realized risks.