**ERP Implementation Risk Assessment Checklist for Internal Auditors**

**(Pre-Work/Planning Phase)**

**Purpose/Scope:** This checklist is designed for Internal Auditors to assess risks during the Pre-Work/Planning phase of an ERP system implementation. It helps to verify that governance structures, risk management strategies, and compliance frameworks are in place before moving to the design and development stages.

**Source**: [CITE SOURCES HERE (E.G. INTERVIEWEES, DOCUMENTS REVIEWED, ETC.]

**Procedures**:

* Assign a risk level to each component to provide context and help prioritize any noted gaps or weaknesses.
* Indicate whether management has met, not met, or partially met the criteria for each component.
* If a component is not applicable, indicate “NA” in the Yes column.
* Maintain this record for regulatory and compliance audits.

**Conclusion:**

[PROVIDE AN OVERALL ASSESSMENT HERE BASED ON THE ANSWERS BELOW]

**Risk Levels:**  
🔴 **High Risk** – Requires immediate mitigation before proceeding to the next phase.  
🟠 **Moderate Risk** – Needs monitoring and mitigation strategies to reduce exposure.  
🟢 **Low Risk** – Adequate controls in place; proceed with implementation.

| **ERP Component** | **Risk** | **Yes** | **No** | **Partial** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| 1. **Governance & Project Oversight Risks** | | | | | |
| * 1. Has a formal project governance framework been established, including an executive steering committee? |  |  |  |  |  |
| * 1. Are key stakeholders (IT, Finance, HR, Compliance, Procurement) actively engaged in the project? |  |  |  |  |  |
| * 1. Has the organization clearly defined roles and responsibilities for project team members, including Internal Audit’s advisory role? |  |  |  |  |  |
| * 1. Is there a detailed project plan with well-defined milestones, deliverables, and timelines? |  |  |  |  |  |
| * 1. Are project risks documented in a risk register, with mitigation strategies assigned? |  |  |  |  |  |
| * 1. Has a change management strategy been developed to manage organizational resistance? |  |  |  |  |  |
| * 1. Is there a vendor selection and evaluation process in place, including background checks and financial stability assessments? |  |  |  |  |  |
| 1. **Business Process Mapping & Change Readiness Risks** | | | | | |
| * 1. Have all key business processes (e.g., finance, HR, procurement, student records) been mapped and documented? |  |  |  |  |  |
| * 1. Are current business processes evaluated for inefficiencies before ERP configuration begins? |  |  |  |  |  |
| * 1. Is there a formalized plan to standardize business processes where possible, rather than over-customizing the ERP system? |  |  |  |  |  |
| * 1. Are existing workflows being reviewed to eliminate redundant or unnecessary steps before automation? |  |  |  |  |  |
| * 1. Has change readiness been assessed among end-users and process owners? |  |  |  |  |  |
| * 1. Are there adequate training and communication plans in place to obtain stakeholder buy-in? |  |  |  |  |  |
| 1. **Data Integrity & Migration Risks** | | | | | |
| * 1. Has a data governance framework been established, including ownership of data across departments? |  |  |  |  |  |
| * 1. Is there a strategy for cleansing, standardizing, and de-duplicating legacy data before migration? |  |  |  |  |  |
| * 1. Have data security and privacy requirements been defined based on regulatory requirements (e.g., GDPR, FERPA, HIPAA)? |  |  |  |  |  |
| * 1. Is there a backup and disaster recovery plan in place for critical data during migration? |  |  |  |  |  |
| * 1. Are controls in place to prevent data corruption or loss during the transition? |  |  |  |  |  |
| * 1. Has data mapping between old and new systems been thoroughly reviewed and approved? |  |  |  |  |  |
| 1. **Risk Assessment & Internal Controls** | | | | | |
| * 1. Has a comprehensive ERP risk assessment been conducted, identifying operational, compliance, and financial risks? |  |  |  |  |  |
| * 1. Are internal controls documented and evaluated to determine whether they will be carried forward or redesigned? |  |  |  |  |  |
| * 1. Has the internal audit function been consulted to provide risk-based insights before implementation? |  |  |  |  |  |
| * 1. Are there documented controls for user access management, segregation of duties (SoD), and privileged access restrictions? |  |  |  |  |  |
| * 1. Are fraud risk controls integrated into the ERP system to prevent unauthorized transactions? |  |  |  |  |  |
| * 1. Is there an audit trail capability within the ERP system to track system changes and financial transactions? |  |  |  |  |  |
| 1. **IT & Cybersecurity Readiness Risks** | | | | | |
| * 1. Have IT security policies been updated to align with ERP implementation requirements? |  |  |  |  |  |
| * 1. Are cybersecurity risks assessed, including vulnerability management and penetration testing? |  |  |  |  |  |
| * 1. Are role-based access controls (RBAC) established to allow least-privilege access? |  |  |  |  |  |
| * 1. Has multi-factor authentication (MFA) been implemented for critical system access? |  |  |  |  |  |
| * 1. Are there encryption policies for data at rest and in transit? |  |  |  |  |  |
| * 1. Has the IT team evaluated disaster recovery and business continuity plans? |  |  |  |  |  |
| 1. **Vendor & Third-Party Risk Management** | | | | | |
| * 1. Have vendor contracts been reviewed to verify that they include security, data privacy, and compliance requirements? |  |  |  |  |  |
| * 1. Are there service-level agreements (SLAs) that outline vendor obligations, system uptime, and support commitments? |  |  |  |  |  |
| * 1. Is there a right-to-audit clause in vendor agreements to allow audits of system performance and security? |  |  |  |  |  |
| * 1. Are third-party integrations reviewed for security vulnerabilities and compatibility with the ERP system? |  |  |  |  |  |
| * 1. Has vendor viability been assessed to mitigate the risk of financial instability or service disruptions? |  |  |  |  |  |
| 1. **Compliance & Regulatory Risks** | | | | | |
| * 1. Are compliance requirements (FERPA, HIPAA, GDPR, SOX, PCI-DSS) considered in system design? |  |  |  |  |  |
| * 1. Have necessary approvals been obtained from regulators or governing bodies? |  |  |  |  |  |
| * 1. Are audit and compliance teams engaged in reviewing the ERP’s compliance capabilities? |  |  |  |  |  |
| * 1. Has a legal review been conducted to confirm that ERP implementation aligns with institutional policies? |  |  |  |  |  |
| 1. **Budget & Financial Planning Risks** | | | | | |
| * 1. Is there a clearly defined budget for ERP implementation, including contingency funds? |  |  |  |  |  |
| * 1. Are cost estimates for licensing, customization, and training realistic? |  |  |  |  |  |
| * 1. Is there a structured approach for tracking and monitoring ERP-related expenses? |  |  |  |  |  |
| * 1. Are financial projections aligned with expected cost savings and operational efficiencies? |  |  |  |  |  |