**Post-Implementation Audit Checklist with Detailed Procedures**
**(For Internal Auditors – ERP Implementation Project)**

**Purpose/Scope:** This checklist is used to conduct a structured post-implementation audit of ERP effectiveness.

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

**Procedures**:

* Most items on this checklist require more detailed testing which should be completed using separate testing work papers.
* Testing work papers and supporting documents should be linked to this checklist using the work paper reference ***(WP Ref)*** column.
* Indicate whether management has met, not met, or partially met the criteria for each component, based on testing procedures performed.
* If a component is not applicable, indicate “NA” in the ***(WP Ref)*** column.
* Maintain this record for regulatory and compliance audits.

**Conclusion:**

**[PROVIDE AN OVERALL ASSESSMENT HERE BASED ON TESTING RESULTS]**

| **Audit Procedure** | **WP Ref** | **Issues**  | **Comments** |
| --- | --- | --- | --- |
| 1. **Project Overview**
 |
| * 1. Obtain and verify the ERP system name, version, go-live date, and any updates from the IT department.
 |  |  |  |
| * 1. Verify if the ERP was rolled out in phases or as a full deployment.
 |  |  |  |
| * 1. List all departments that have transitioned to the ERP system.
 |  |  |  |
| * 1. Define the Scope of the Review (finance, HR, student services, etc.)
 |  |  |  |
| * 1. List primary objectives of the ERP implementation. Compare stated objectives against the actual implemented functionalities.
 |  |  |  |
| * 1. Review project charters and business case documents.
 |  |  |  |
| 1. **System Performance & Functionality**
 |
| * 1. Obtain system uptime reports from IT and verify against agreed Service Level Agreements (SLAs).
 |  |  |  |
| * 1. Interview IT personnel to determine frequency and causes of system downtime.
 |  |  |  |
| * 1. Select and review a sample of transactions processed post-implementation (financial transactions, payroll, student records) and verify that they were processed timely and accurately.
 |  |  |  |
| * 1. Reconcile financial transactions with ledger records and bank statements.
 |  |  |  |
| * 1. Compare a random sample of pre- and post-migration data sets **(financial, student, HR data)**
 |  |  |  |
| * 1. Verify completeness by ensuring all historical data is accessible and accurate.
 |  |  |  |
| * 1. Review IT helpdesk tickets related to ERP errors and classify them by frequency and severity.
 |  |  |  |
| * 1. Select a sample and validate if previously reported issues were resolved within defined timelines.
 |  |  |  |
| * 1. Conduct real-time system performance tests with the IT department.
 |  |  |  |
| * 1. Compare system response times before and after implementation.
 |  |  |  |
| 1. **Compliance & Security Review**
 |
| * 1. Cross-check system configurations against regulatory requirements (FERPA, HEA, PCI DSS, GDPR, OMB Uniform Guidance)
 |  |  |  |
| * 1. Review audit logs to confirm adherence to data privacy standards.
 |  |  |  |
| * 1. Extract and analyze a list of user roles and permissions from the ERP system. Test a sample of transactions to confirm no single user has conflicting privileges.
 |  |  |  |
| * 1. Review encryption methods, authentication protocols, and security certificates applied to sensitive data.
 |  |  |  |
| * 1. Conduct an IT security assessment to identify unauthorized access attempts.
 |  |  |  |
| * 1. Review ERP system logs for completeness, timestamp accuracy, and modification history.
 |  |  |  |
| * 1. Verify that log retention policies meet institutional and regulatory standards.
 |  |  |  |
| 1. **User Adoption & Training Effectiveness**
 |
| * 1. Distribute post-implementation user surveys and analyze feedback trends. Identify and escalate unresolved issues to IT or project teams.
 |  |  |  |
| * 1. Extract and categorize support tickets by issue type and department. Identify trends indicating training gaps or system weaknesses.Obtain training attendance records and verify against ERP access logs.
 |  |  |  |
| * 1. Interview department managers to assess staff readiness and knowledge gaps.
 |  |  |  |
| * 1. Recommend additional training modules based on audit findings.
 |  |  |  |
| 1. **Change Management & Issue Resolution**
 |
| * 1. Review change request logs and verify against formal approval workflows. Ensure changes did not bypass required approvals.
 |  |  |  |
| * 1. Retrieve and evaluate outstanding customization requests. Determine if requests align with strategic business needs.
 |  |  |  |
| * 1. Compare baseline process efficiency metrics pre- and post-ERP implementation. Identify bottlenecks that may still require optimization.
 |  |  |  |
| * 1. Document key lessons learned from project teams and system users. Recommend corrective actions for future ERP optimizations, as needed.
 |  |  |  |
| 1. **Business Continuity & Disaster Recovery Assessment**
 |
| * 1. Test backup restoration procedures for critical financial and student data.
 |  |  |  |
| * 1. Verify backup logs for completeness and successful execution.
 |  |  |  |
| * 1. Evaluate incident response logs and resolution times.
 |  |  |  |
| * 1. Ensure communication protocols are effective during system disruptions.
 |  |  |  |
| * 1. Conduct system failover testing with IT teams.
 |  |  |  |
| * 1. Assess redundancy measures to confirm continuous service availability.
 |  |  |  |
| 1. **Lessons Learned & Recommendations for Future Improvements**
 |
| * 1. Compile a report on implementation successes and benefits realized.
 |  |  |  |
| * 1. List key system enhancements required for better efficiency.
 |  |  |  |
| * 1. Highlight ongoing risks that require continuous monitoring.
 |  |  |  |
| * 1. Define clear corrective actions with assigned ownership and timelines.
 |  |  |  |