**Change Control Procedures Checklist**
**(For Internal Auditors – Design Phase of ERP Implementation)**

**Purpose/Scope**: This checklist helps auditors verify that management has implemented the proper policies, procedures and controls so that changes to the ERP system during the Design Phase are properly evaluated, documented, tested, and approved to prevent security, compliance, and operational risks.

**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.

| **Change Component** | **Risk** | **Yes** | **No** | **Partial** | **Comments** |
| --- | --- | --- | --- | --- | --- |
| 1. **Governance & Oversight**
 |  |  |  |  |  |
| 1. **Formal Change Management Policy:** Documented policy outlining roles, responsibilities, and approval workflows.
 |  |  |  |  |  |
| 1. **Change Control Committee:** Cross-functional review board (CRB) with representatives from finance, IT, compliance, and audit.
 |  |  |  |  |  |
| 1. **Approval Authority Levels:** Defined approval hierarchy for different types of changes.
 |  |  |  |  |  |
| 1. **Change Classification:** Categorization of changes (standard, emergency, major) with appropriate approval protocols.
 |  |  |  |  |  |
| 1. **Change Request & Documentation**
 |  |  |  |  |  |
| 1. **Formal Change Request Process:** Standardized Change Request Form (CRF) for logging all requests.
 |  |  |  |  |  |
| 1. **Change Justification:** Business rationale, impact analysis, and risk assessment documented for each change.
 |  |  |  |  |  |
| 1. **Stakeholder Notification:** Communication plan to inform affected faculty, staff, and IT personnel.
 |  |  |  |  |  |
| 1. **Version Control & Audit Trail:** Management maintains timestamped logs of all changes for tracking and compliance.
 |  |  |  |  |  |
| 1. **Risk Assessment & Compliance Checks**
 |  |  |  |  |  |
| 1. **Security & Data Privacy Impact Assessment:** Management has assessed system requirements needed to comply with FERPA, HEA, GDPR, and other regulations.
 |  |  |  |  |  |
| 1. **Segregation of Duties (SoD) Review:** Management has reviewed access controls to prevent conflicts in system roles.
 |  |  |  |  |  |
| 1. **Financial & Operational Risks:** Management has conducted a disruption of service impact assessment on tuition, payroll, financial aid, and grants.
 |  |  |  |  |  |
| 1. **Disaster Recovery & Contingency Planning:** Management has rollback procedures in case of system failure or negative impacts.
 |  |  |  |  |  |
| 1. **Testing & User Acceptance**
 |  |  |  |  |  |
| 1. **Test Environment Validation:** Management tests changes in a non-production (sandbox) environment.
 |  |  |  |  |  |
| 1. **User Acceptance Testing (UAT):** End-users (finance, faculty, IT) have successfully tested changes.
 |  |  |  |  |  |
| 1. **System Integration Testing:** Management verifies that changes do not break integrations with financial and student information systems.
 |  |  |  |  |  |
| 1. **Performance Testing: Management has mechanisms to assess** system speed, reporting, and data processing against contractual requirements.
 |  |  |  |  |  |
| 1. **Approval & Implementation Controls**
 |  |  |  |  |  |
| 1. **Final Approval Documentation:** Written approval is obtained from senior management before deployment.
 |  |  |  |  |  |
| 1. **Scheduled Deployment:** Implementation is scheduled during low-impact periods (e.g., outside registration or fiscal year-end).
 |  |  |  |  |  |
| 1. **Access & Security Adjustments:** Compliance with role-based access control (RBAC) policies.
 |  |  |  |  |  |
| 1. **End-User Training & Communication:** Proper training for employees before deployment.
 |  |  |  |  |  |
| 1. **Post-Implementation Monitoring & Audit**
 |  |  |  |  |  |
| 1. **Change Effectiveness Review:** Post-implementation audit is scheduled and budgeted to assess success and operational impact.
 |  |  |  |  |  |
| 1. **Error/Incident Logging:** Tracking mechanisms are in place to monitor/report unexpected issues and resolutions.
 |  |  |  |  |  |
| 1. **Audit Trail Verification:** ERP system maintains records of all approved and implemented changes.
 |  |  |  |  |  |