RISK MATRIX

PURPOSE

This matrix defines the risk levels for exceptions identified during the lab, providing a consistent basis for rating issues.

RISK LEVELS & CRITERIA:

A. HIGH RISK (Severe Impact — Immediate Action Required):

1. **Criteria:**
   - Terminated employees still have Active accounts in the Critical ERP System.
   - Privileged/Admin access without proper approval.
   - Role assignments inconsistent with job role (with privileged right).
   - Any gap that could allow unauthorized transactions in a critical system.
   - Missing Ticket or Approval Email for provisioning or modification of users with Editor, Approver and Admin Roles (Rights).
   - Termination disablement more than 1 business day late.

2. **Impact:**
   - Direct opportunity for fraud or data breach.
   - Regulatory non-compliance (e.g., SOX, GDPR).

3. **Recommended Action:**
   - Immediate removal of access; review similar accounts.

B. MEDIUM RISK (Moderate Impact — Prompt Remediation):

1. **Criteria:**
   - Missing Ticket or Approval Email for provisioning or modification of users with Viewer Roles (Rights).
   - Role assignments inconsistent with job role but not privileged.

2. **Impact:**

- Increased potential for unauthorized access if combined with other weaknesses.

3. **Recommended Action:**
   - Reinforce approval requirements; implement automated alerts.

C. **LOW RISK (Low Impact — Monitor):**

1. **Criteria:**
   - Minor documentation gaps where control outcome was still achieved.
   - Incomplete ticket closure notes, but disablement/approval occurred.

2. **Impact:**
   - Minimal risk in isolation. It can erode control discipline if persistent.

3. **Recommended Action:**
   - Address process consistency in next team meeting.