System Audit Report

Overall Score: 3.4 / 5.0

Date: 2026-01-19

Risk Level: High

Scope: Full System

1. Dimension Scores

Dimension	Score	Findings
Code Quality	5.0	0
Security	5.0	0
Testing	0.0	1
Database	5.0	11
API	0.5	1
Architecture	5.0	0
UI/UX	5.0	0
AI Layer	5.0	8
DevOps	1.5	3
Drift Detection	0.0	14
Performance	5.0	0

2. Critical Findings

[Critical] No Prompt Injection Protection Detected

Description: AI system lacks input sanitization to prevent prompt injection attacks.
Recommendation: Implement input sanitization/escaping before incorporating user input into prompts.

[Critical] No backup strategy implemented

Description: Database backup scripts not found
Recommendation: Implement automated database backup mechanism

3. Major Findings

[Major] Test coverage estimated at 28.5%

Description: Low test coverage detected
Recommendation: Add unit tests for core modules

[Major] Unenforced Foreign Key: 'core_organizations.head_id'

Description: Column 'head_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for head_id

[Major] Unenforced Foreign Key: 'core_organizations.tax_id'

Description: Column 'tax_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for tax_id

[Major] Unenforced Foreign Key: 'core_users.employee_id'

Description: Column 'employee_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for employee_id

[Major] Unenforced Foreign Key: 'core_departments.hod_id'

Description: Column 'hod_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for hod_id

[Major] Unenforced Foreign Key: 'core_departments.manager_id'

Description: Column 'manager_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for manager_id

[Major] Unenforced Foreign Key: 'core_sub_departments.manager_id'

Description: Column 'manager_id' suggests a relation but has no FK constraint.
Recommendation: Add FOREIGN KEY constraint for manager_id

[Major] Insufficient input validation on AI calls

Description: Not all AI integrations validate input data (8/53)
Recommendation: Add schema validation before sending data to AI models

[Major] Unsafe AI Temperature Settings

Description: Found 46 AI calls without explicit low-temperature settings (risk of hallucinations).
Recommendation: Set temperature=0.0-0.2 for factual tasks.

[Major] Missing Grounding Instructions

Description: Found 52 AI prompts without grounding constraints.
Recommendation: Include 'only use provided context' or similar constraints in prompts.

[Major] Missing Response Validation

Description: Found 50 AI calls without response validation.
Recommendation: Implement schema validation or parsing for AI outputs to catch malformed responses.

[Major] No PII Redaction Detected

Description: AI system doesn't appear to redact sensitive data before sending to external APIs.
Recommendation: Implement PII detection and redaction (e.g., using Presidio or scrubadub).

[Major] Insufficient Fallback Behavior

Description: Less than 50% of AI calls have fallback logic (0/53).
Recommendation: Implement graceful degradation with default responses when AI calls fail.

[Major] No deployment scripts found

Description: Missing automated deployment configuration
Recommendation: Create deployment scripts (start_app.bat/sh, Dockerfile)

4. Action Plan

Issue	Owner	Priority
No Prompt Injection Protection Detected	unassigned	Critical
No backup strategy implemented	unassigned	Critical
Test coverage estimated at 28.5%	unassigned	High
Unenforced Foreign Key: 'core_organizations.h	unassigned	High
Unenforced Foreign Key: 'core_organizations.t	unassigned	High
Unenforced Foreign Key: 'core_users.employee_	unassigned	High
Unenforced Foreign Key: 'core_departments.hod	unassigned	High
Unenforced Foreign Key: 'core_departments.man	unassigned	High
Unenforced Foreign Key: 'core_sub_departments	unassigned	High
Insufficient input validation on AI calls	unassigned	High