Final Audit Report

IT General Controls (ITGC) – Healthcare Portfolio Engagement

Date: 2025-12-27

Organization: Jacob’s Dome (Fictional)

Systems: HR System; Medical Records System

1. Executive Summary

This simulated ITGC audit evaluated controls across Access Controls, Change Management, and IT Operations. Two High-Risk findings were identified in access deprovisioning and change management, alongside one Medium-Risk finding in access provisioning and one observation related to log review execution.

2. Overall Assessment

Area	Overall Result	Rationale (Condensed)
Access Controls	Needs Improvement	Termination access removal failures including retained admin access.
Change Management	Unsatisfactory	Unapproved production changes and weak emergency change follow-up/testing.
IT Operations	Needs Improvement	One missed log review period; incident handling performed appropriately.

3. Summary of Findings

ID	Control	Severity	Issue
F-01	AC-02 Deprovisioning	High	Terminated users retained access; one retained admin access.
F-02	CM-01 Change Approval	High	Unapproved production changes; emergency change reviewed late without tes
F-03	AC-01 Provisioning	Medium	Access granted without documented approval evidence.
O-01	OP-03 Log Review	Observation	One missed review period; exception ticket handled within timeframe.

F-01 — Failure to Timely Remove Access for Terminated Employees (High)

Condition: Two terminated users retained active access beyond termination dates; one retained administrator-level access.

Criteria: Access Control Policy requires removal of system access within 24 hours of termination.

Cause: HR-to-IT offboarding workflow is not effectively enforced and termination notifications are not consistently processed.

Effect / Risk: Increases risk of unauthorized access, PHI exposure, payroll manipulation, and malicious or accidental changes; retained admin access materially increases compromise risk.

Recommendation: Implement automated HR-to-IT offboarding, remediate active terminated accounts immediately, and perform retrospective log/change review for the exposure window.

F-02 — Unapproved and Improperly Reviewed Changes Implemented in Production (High)

Condition: Two production changes to the Medical Records System were implemented without documented approval. One emergency change was reviewed five days post-implementation with no evidence of post-implementation testing.

Criteria: Change Management Policy requires approvals prior to implementation and timely review/testing for emergency changes per SLAs.

Cause: Change governance is not consistently enforced; preventive controls do not reliably block deployment without authorization; emergency follow-up is not monitored.

Effect / Risk: Unapproved/untested changes increase risk of downtime, integrity issues in medical records, and compliance exposure; in healthcare this may affect patient care and data reliability.

Recommendation: Enforce approval gates (technical and procedural), require testing evidence, strengthen emergency review SLAs with monitoring, and track remediation to closure.

F-03 — User Access Provisioned Without Documented Approval (Medium)

Condition: Two users were provisioned access without documented approval from the data owner, though access levels generally aligned with job roles.

Criteria: Access provisioning requires documented authorization and least privilege alignment.

Cause: Provisioning workflow enforcement and evidence retention are inconsistent.

Effect / Risk: Reduces assurance that access is appropriately authorized; increases risk of unauthorized access and privilege creep over time.

Recommendation: Mandate approval evidence prior to provisioning, perform retrospective review of recent access grants, and implement workflow checks that prevent provisioning without recorded authorization.

O-01 — Inconsistent Execution of Log Reviews (Observation)

Condition: One scheduled log review period was missed; an exception for multiple failed login attempts was logged and handled within the expected timeframe.

Criteria: Monitoring procedures require periodic log reviews and evidence retention.

Cause: Review cadence enforcement is inconsistent.

Effect / Risk: May delay detection of suspicious activity during missed periods.

Recommendation: Reinforce review cadence, clarify accountability, and retain evidence of completion for each review period.

4. Follow-Up Plan

Perform a follow-up review within 90 days to validate remediation of High-Risk findings (F-01, F-02) and confirm that Medium-Risk actions (F-03) and observation items (O-01) are addressed.

Note: This portfolio engagement uses fictional data and does not include real PHI or employee information.