# Audit Plan

## IT General Controls (ITGC) – Healthcare Portfolio Engagement

**Date:** 2025-12-27

**Engagement Type:** Simulated Internal Audit (Portfolio)

**Organization:** Jacob's Dome (Fictional) – Healthcare, 75 employees, 2 key systems

## 1. Objective

Evaluate the design and operating effectiveness of IT General Controls supporting the HR System and Medical Records System to provide assurance over confidentiality, integrity, and availability (CIA).

## 2. Scope

| In Scope | Details |
|---|---|
| Systems | HR System; Medical Records System |
| Domains | Access Controls (AC), Change Management (CM), IT Operations (OP) |
| Time Period | Last 6 months (simulated evidence set) |

**Out of Scope:** application functionality/clinical workflows; financial reporting accuracy; penetration testing.

## 3. Risk Focus

Primary risks assessed include unauthorized access (including excessive privilege), payroll manipulation, PHI exposure, unapproved changes impacting system integrity, and inadequate monitoring/log review execution.

## 4. Methodology

• Risk-based planning and control mapping (COBIT, ISO/IEC 27001, COSO referenced).

• Design effectiveness assessment: confirm control intent, ownership, frequency, and evidence requirements.

• Operating effectiveness testing: inspection/inquiry using samples from recent activity; document exceptions.

• Issue evaluation: assess frequency (pattern), system criticality, and potential impact to determine severity.

• Reporting: condition/criteria/cause/effect/recommendation with remediation actions and follow-up cadence.

## 5. Planned Tests (Summary)

| Control | Test Objective | Sample / Evidence |
|---|---|---|
| AC-01 Provisioning | Verify documented approvals prior to granting access | 10 active users; request/approval evidence |
| AC-02 Deprovisioning | Verify access removal within 24 hours of termination | 5 terminations; disablement records |

| | | |
|---|---|---|
| CM-01 Change Approval | Verify approvals and emergency review/testing | 5 production changes; tickets/approvals |
| OP-03 Log Review | Verify log review cadence and evidence | Review schedule + exception handling evidence |

## 6. Deliverables

• Audit plan and workpapers (risk matrix, controls matrix, findings register)

• Final ITGC audit report (executive summary, findings, remediation recommendations)

• Follow-up plan (90-day validation for High-Risk findings)

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