Internal Audit Report: User Access Control

Company: Carraway IT Consultants

To: Chief Information Security Officer (CISO)

From: Tia Mitchell, GRC Analyst

Date: January 2026

Subject: Quarterly Access Review – Production Database

1. Executive Summary

The internal audit of Access Controls for the Production Database resulted in a rating of Needs Improvement. We identified five (5) high-risk findings that currently expose the organization to unauthorized data access and potential regulatory non-compliance. Aligning the identity and access management (IAM) lifecycle with NIST SP 800-53 and ISO 27001 standards is required to remediate these gaps and ensure the integrity of business operations.

2. Scope of Review

The scope included a point-in-time review of all user accounts associated with the Production Database. The audit compared active system accounts against HR employment records and the internal Role-Based Access Control (RBAC) matrix to verify the Principle of Least Privilege (PoLP) and the effectiveness of account deprovisioning.

3. Summary of Findings

Finding ID	Risk Level	Title	Description
01	**High**	Orphaned Accounts	Two (2) accounts (Alice, Bob) remain "Active" despite employee termination.
02	**Medium**	Privilege Creep	Admin-level access was identified for non-DevOps roles (Developer, Intern).
03	**High**	Control Failure	Failure in the deprovisioning workflow between HR and IT Departments.

User Name	Role	Access Level	Status	Observation	Recommended Action
Sarah	DevOps	Admin	Active	Satisfactory	No action required.
Mike	Developer	Admin	Active	Privilege Creep	Downgrade to 'User' access.
Bob	(Term)	User	Active	Orphaned Account	**Immediate Deactivation**
Alice	(Term)	Admin	Active	Critical Risk	**Immediate Deactivation**
Leo	Intern	Admin	Active	PoLP Violation	Downgrade to 'User' access.

4. Root Cause Analysis

The audit identified a breakdown in the Joiner-Mover-Leaver (JML) process. Specifically:

- **Communication Gap:** A lack of automated notification between HR and IT resulted in delayed account deactivation.
- **Lack of Automated Provisioning:** System access levels are manually assigned, without automated guardrails, allowing roles such as “intern” to inherit “Admin” permissions.

5. Management Action Plan

1. **Immediate Terminations:** All orphaned accounts (Alice, Bob) must be deactivated by EOD today.
2. **Access Recertification:** IT must perform a full review of all Admin permissions by February 20, 2026, to ensure alignment with the RBAC matrix
3. **Process Improvement:** Implement an automated ticketing trigger between HR software and Active Directory to ensure deprovisioning occurs within 24 hours of termination.

***NOTE:** A follow-up “Audit of the Audit” will be scheduled for February 20, 2026, to verify that the remediation steps have been successfully implemented and that the orphaned accounts remain disabled.