Internal Audit Report: Employee Lifecycle and Payroll Integrity

Executive Summary

The audit objective was to evaluate the controls governing employee onboarding, termination, and payroll data accuracy. We discovered critical failures in the communication bridge between HR and IT, leading to 'ghost employees' remaining active in the payroll system post-resignation. The control environment is currently deemed unsatisfactory.

Risk Assessment & In-Depth Analysis

Risk 1: Delayed Termination Processing — Rating: Very severe risk
In-Depth Analysis: Systemic delays in notifying the payroll department of employee departures have resulted in unauthorized salary payments. We have quantified a direct loss of $485,000 in overpayments to 12 former employees who remained on the active payroll for an average of three months post-termination. This reflects a breakdown in fundamental administrative synchronization.

Risk 2: PII Data Leakage — Rating: Average-high risk
In-Depth Analysis: Employee Personally Identifiable Information (PII) is frequently shared via unencrypted email attachments during the benefits enrollment process. This exposes the firm to significant data breach liability and potential fines under GDPR and CCPA. The lack of a secure document transfer protocol is a primary driver of this risk.

Audit Findings

Finding 1: Inactive User Access
Over 50 terminated employees still possessed active VPN and internal database credentials, posing a massive security risk to corporate intellectual property.

Finding 2: Inconsistent Payroll Reconciliation
Monthly payroll registers are being approved without a line-by-line reconciliation against the HRIS headcount report, allowing discrepancies to go undetected for multiple cycles.

Recommendations

Recommendation 1: Automated Termination Workflow
HR must implement an automated notification trigger in the HRIS that simultaneously alerts Payroll, IT, and Facilities when a termination date is entered, ensuring immediate cessation of pay and access.

Recommendation 2: Mandatory Use of Secure File Transfer
The use of email for transmitting PII must be prohibited immediately, with all sensitive data transfers required to occur via the company's secure, encrypted portal.

Management Response

Management partially disagrees with the severity of Finding 1. While we acknowledge the delay in access revocation, we believe the risk to intellectual property is overstated as no unauthorized data egress was detected during the period in question. We also maintain that the $485,000 figure includes several disputed severance payments which we intend to claw back, thus reducing the actual loss.

Conclusion

Significant residual risk exists regarding payroll integrity and data security. Management must prioritize the synchronization of HR and IT systems to prevent further financial leakage and potential data compromises.