PayrollCo – Risk Determination & Monitoring Report

Vendor: PayrollCo

Service: Payroll Processing SaaS

Data Classification: Regulated (Employee PII – SSN, Banking Data)

Assessment Date: February 26, 2026

Assessor: GRC Analyst (Portfolio Simulation)

1. Findings Summary

Finding ID	Control Domain	Severity	Description	Remediation Target
F-001	Logging & Monitoring	High	Audit logs retained only 7 days; no centralized SIEM export.	May 31, 2026
F-002	Subprocessor Management	Medium	No formal subprocessor change notification process documented.	June 30, 2026
F-003	Vulnerability Management	Medium	Patch SLA documentation incomplete; remediation timelines unclear.	May 15, 2026

Impact Summary:

The primary risk driver is insufficient logging retention, which may impair incident detection and forensic investigation capability. Subprocessor transparency and incomplete patch governance introduce moderate supply chain and operational risk.

2. Residual Risk Determination

Inherent Risk Level: HIGH

Control Strength Assessment: Moderately Effective

Open High Severity Findings: 1

Open Medium Severity Findings: 2

Residual Risk Rating: HIGH

Residual risk remains HIGH due to the unresolved High severity logging gap. While core security controls (MFA, encryption, IR plan, DR testing) are in place, monitoring weaknesses increase the likelihood of delayed breach detection.

3. Risk Decision

Decision: APPROVE WITH CONDITIONS

Conditions for Approval:

- Extend audit log retention to a minimum of 90 days OR enable SIEM export.
- Provide documented subprocessor notification procedure.
- Formalize and document patch management SLA.
- Provide remediation evidence prior to next quarterly review.

Executive approval not required at this time; conditional approval granted pending remediation validation.

4. Ongoing Monitoring Plan

- Quarterly review of remediation progress.
- Annual SOC 2 Type II report review upon issuance.
- Notification of material subprocessor changes.
- Annual reassessment of inherent and residual risk.
- Immediate reassessment upon security incident disclosure.

Monitoring Frequency: Quarterly until all High findings are closed, then Semiannual thereafter.

Prepared by: ________________________

Approved by: ________________________

Date: ______________________________

Created by: Jodelis Diaz