

Third-Party Risk Assessment Report

Vendor: PayrollCo

Assessment Type: New Vendor Assessment

1. Vendor Intake & Classification

- Service Provided: Payroll Processing SaaS
- Business Owner: HR Director
- Data Classification: Regulated (Employee PII: SSN, banking data)
- Access Level: API integration with HRIS and banking systems
- Business Criticality: High – Payroll processing is operationally critical
- Regulatory Impact: SOC 2, ISO 27001 supplier controls applicable

2. Inherent Risk Assessment

Based on data sensitivity (regulated PII), API integration, and high business criticality, the vendor is classified as HIGH inherent risk.

3. Due Diligence Review

- Reviewed SOC 2 Type II report (Security & Availability criteria).
- Validated encryption at rest and in transit.
- Confirmed incident response plan and breach notification commitment (≤ 72 hours).
- Reviewed disaster recovery testing summary (annual testing performed).
- Identified logging retention gap (7 days only).
- Subprocessor transparency documentation incomplete.

4. Findings Summary

Finding ID	Severity	Description	Status
F-001	High	Audit logs retained only 7 days; no SIEM export	Open
F-002	Medium	No formal subprocessor notification process	Open

5. Residual Risk Determination

Due to open High severity findings related to logging and monitoring, residual risk remains HIGH until remediation is verified.

6. Risk Decision

- Decision: Approve with Conditions

- Condition 1: Extend log retention to minimum 90 days or enable SIEM export.
- Condition 2: Provide documented subprocessor notification process.
- Review Frequency: Quarterly until remediation closure.

Prepared by: GRC Analyst Jodelis Diaz