2026 | By: Ifeanyi Ijezie

AtlasPay Risk Audit

In-depth look at Risks & Vulnerabilities

AtlasPay

Risk Management Audit

Overview

AtlasPay processes payments and stores sensitive customer and financial data. The company recently experienced a phishing incident involving an employee in the finance department. Company executives are concerned about regulatory exposure, weak documentation, and unclear ownership of controls.

A risk assessment is required to understand security and compliance risks prior to SOC 2 readiness.

Objectives

- Risk Assessment
- Risk Register
- Heat Map
- Treatment Options and Recommendations
- Gap analysis
- Documentation

Frameworks that will be referenced:

- NIST CFS
- NIST SP 800-53 Rev. 5

Executive Summary

AtlasPay Solutions processes payment transactions and maintains sensitive customer and financial data, requiring a strong and well-documented security and risk management posture. Following a recent phishing incident within the finance department, executive leadership identified the need to formally assess security, compliance, and governance risks in preparation for SOC 2 readiness. A comprehensive risk assessment was performed using NIST-aligned frameworks, including the NIST Cybersecurity Framework and NIST SP 800-53, to identify, analyze, and prioritize key risks across the organization. The assessment produced a structured risk register, heat map, gap analysis, and treatment recommendations, highlighting elevated risk in areas such as phishing, access control, incident response readiness, third-party oversight, logging and monitoring, and security awareness. While several controls are in place, targeted improvements in documentation, ownership, and control effectiveness are necessary to reduce exposure and support ongoing compliance objectives.

Impact Statement

Effective risk management is essential to AtlasPay's ability to protect revenue, control costs, and maintain trust with customers, partners, and regulators. As a payment processing organization handling sensitive financial and customer data, security incidents such as phishing, unauthorized access, or third-party breaches can result in direct financial losses through fraud, service disruption, regulatory penalties, and customer attrition. By conducting a structured risk assessment, AtlasPay gains visibility into where these financial exposures exist and how likely they are to materialize, allowing leadership to proactively address risks before they escalate into costly incidents.

Beyond loss prevention, this assessment enables AtlasPay to make informed, profit-protective decisions by prioritizing investments where they deliver the highest return. Rather than allocating resources reactively or evenly across all areas, leadership can focus remediation efforts on risks with the greatest potential financial and operational impact. Aligning risk treatment decisions with quantified impact and likelihood ensures that security spending supports business objectives, reduces unnecessary control overhead, and avoids inefficient or redundant investments that do not materially reduce risk.

Finally, acting on the findings of this assessment strengthens AtlasPay's long-term financial position by supporting audit readiness, customer confidence, and market credibility. Demonstrating a mature, NIST-aligned risk management program reduces the likelihood of failed audits, delayed deals, increased insurance premiums, or contractual penalties tied to security deficiencies. By integrating risk management into strategic decision-making, AtlasPay not only minimizes potential losses but also protects revenue growth, improves operational efficiency, and reinforces its reputation as a trustworthy financial services provider.

Risk Assessment

This risk assessment was conducted using a NIST SP 800-53 Rev. 5 aligned methodology to identify, evaluate, and prioritize key information security and operational risks across the organization. The assessment evaluated inherent and residual risk by applying a quantitative impact and likelihood model to ensure consistent and repeatable risk scoring. Six primary risks were identified, with the highest exposures related to phishing, access control weaknesses, incident response readiness, and third-party vendor oversight. While several baseline controls are in place, multiple risks were determined to be only partially mitigated due to gaps in governance, monitoring, and formalized processes. Recommended mitigation actions focus on strengthening preventive and detective controls, improving incident preparedness, and enhancing oversight of privileged access and third-party relationships. Overall, the organization's risk posture is manageable, but targeted improvements are required to reduce the likelihood and impact of high-risk scenarios.

Risk Assessment
Used to identify, assess, and take action regarding risk

IJEZIE RISK ADVISORY

Compnay Name: AtlasPay
Administrative Structure:
Completed By: Ifeanyi Ijezie
Date Completed: 1/1/26
Date of Next Risk: 4/1/26

Click to update Heat Map

Business Objective AtlasPay processes payments and stores sensitive customer and financial data. A risk assessment is required to understand security and compliance risks prior to SOC 2 readiness.

What is the risk?	Risk Category	Existing Controls	Comments/Concerns	mpact(Inherent	Likelihood(Inherent)	Risk Calculation Impact	Likelihood	Risk Score	Stakeholders	Recommended Risk Treatment Actions	Which Management Strategy? (mitigate, transfer, avoid, accept)	Responsible Person/Job Title	Target Completion Date
R-01 (Phishing attacks)	Operational	Email filtering, annuak security awareness training	No phishing program in place, Multi-factor auth not enforced for all privl. Or finance users, Training frequency not sufficient for remote work	Catastrophic	High	5	5	25	IT Security, Fincance Leadership, Compliance/Risk Management	enforce MFA, Impliment quarterly phishing simulation, Enhance monitoring and aleting for sus login activity	Mitigate	Director of IT Secutity	90 Days from assessment
R-02 (Access Controls)	Technical	Role based access is infitmally applied, Access granted upon IT request, Account disabled when employee leaves	No formal access reviews are conducged, Privileged accounts are not consistently identified/tracked, Access approvals are not documented, Least privileged is not enforced consistently	Significant	Medium	4	3	12	IT Security, System Owners, Human Resources, Compliance/Risk Management	Quarterly user access reviews for critical systems, Impliment formal role based access definitions, Identify and track all privileged accounts, Require docummted approval for access changes	Mitigate	IT Security Manager	120 days from assessment
R-03 (Log & monitor)	Technical	System Logs are enabled on critical systems, Logs are retained for a limited period, Alerts are generated for some security events	Logs are not reviewed on a regular basis, No centralized log management solutions are in place, Alerting thresholds may not cover all high risk activities, Incident response relies heavily on manual detection	Moderate	Medium	3	3	9	IT Security, System Admins, Compliance/Management	Implement centralized log aggregation and monitoring, Define and document log review procedures, Establish alerting for high risk events. (failed logins,privilege changes)	Mitigate	IT Security Operations Lead	90 Days from assessment
R-04 (IR and testing)	Managerial	IR plan is in draft or informal form, Roles and responsibilities are loosely defined, Incidents are handled on an ad hoc basis	IR plan has not been formally approved, No tabletop exercises or simulations have been conducted, Employees may be unclear on escalation proceedures, Lessons learned are not formally documented	Significant	Medium	4	3	12	IT Security, Executive Management, Legal/Compliance, Communications/Public Sector	Finalize and formally approve the incident response plan, Define clear IR roles and escalation paths, Conduct annual tabletop IR excersises, Document lessons learned and update procedures accordingly	Mitigate	CISO	120 days from assessment
R-05 (Vendor Risk)	Third Party	Vendors are selected based on business need, Controls include basic confidentiality clasues, IT involvement in vendor onboarding is informal	No formal vendor risk assessment process, Security requirements are not consistently documented, Vendor access is not preiodically viewed, No process for reassessing vendors after onboarding	Catastrophic	Medium	5	3	15	Vendor Management, IT Security, Legal/Compliance, Business Unit Owners	Establish formal third-party risk management process, Require security questions during onboarding, Define minimum security requirements for vendors, Conduct periodic reviews of high-risk vendors	Mitigate	Vendor Risk Manager	150 Days from assessment
R-06 (Sec Training)	Operational	Provided annually, New employees receive basic onboarding guidance, Policies are available to employees upon request	Not enough training for the threat landscape, No role based or targeted trainng for high-risk users, Effectiveness is not measured, Employees may not fully understand reporting procedures	Mild	High	2	5	10	IT Security, HR, Compliance/Risk Management	Impliment role-based security training, Conduct periodic simulations, Track and report training completion metrics, Reinforce incident reporting procedures	Mitigate	Security Awareness Program Manager	90 Days from assessment

Assessment Scope

This assessment focused on systems, processes, and personnel involved in payment processing, financial operations, and supporting information systems, including access management, monitoring, incident response, and third-party interactions.

Methodology Summary

- Risks were identified based on threat, vulnerability, and potential business impact.
- Inherent and residual risk were calculated using a quantitative impact and likelihood scoring model.
- Identified risks were mapped to applicable NIST SP 800-53 Rev. 5 control families to evaluate control effectiveness and gaps.

Risk Register Overview

The risk register consolidates all identified risks from the assessment into a single, structured view to support accountability, tracking, and decision-making. Each risk is documented with defined ownership, inherent and residual risk ratings, selected treatment strategies, and target remediation timelines. The register serves as a living management tool, allowing leadership to monitor risk status, evaluate progress on mitigation efforts, and reassess risk levels as controls are implemented. Risk scores within the register are calculated using a NIST-aligned quantitative impact and likelihood model to ensure consistency across the organization. This approach enables leadership to prioritize remediation activities based on risk severity and business impact.

Risk Register

Company Name: AtlasPay
Administrative Structure: 0
Completed By: Ifeanyi Ijezie
Date: 1/1/2026
Date of Next Risk Assessment: 4/1/2026

IJEZIE RISK ADVISORY

Identified Risk	Actions to address the risk	Responsible Person/Job Title	Updates/Status	Target Completion Date	Actual Completion Date	Impact	Likelihood	Risk Calculation Comparison	
								Risk Score (Original)	Risk Score (Residual)
R-01 (Phishing attacks)	enforce MFA, Impliment quarterly phishing simulation, Enhance monitoring and aleting for sus login activity	Director of IT Secutity	Completed – MFA enforced for all finance and privileged users; phishing simulations implemented and completed.	90 Days from assessment	3/31/2026	Moderate	Low	20	3
R-02 (Access Controls)	Quarterly user access reviews for critical systems, Impliment formal role based access definitions, Identify and track all privileged accounts, Require documrnted approval for access changes	IT Security Manager	In progress – access review process being defined; role-based access documentation in draft.	120 days from assessment				12	#N/A
R-03 (Log & monitor)	Implement centralized log aggregation and monitoring, Define and document log review procedures, Establish alerting for high risk events. (failed logins,priviege changes)	IT Security Operations Lead	Planned – evaluating SIEM/log aggregation options and alerting requirements.	90 Days from assessment				9	#N/A
R-04 (IR and testing)	Finalize and formally approve the incident response plan, Define clear IR roles and escalation paths, Conduct annual tabletop IR excersises, Document lessons learned and update procedures accordingly	CISO	Planned – incident response plan pending executive approval; tabletop exercise scheduled.	120 days from assessment				12	#N/A
R-05 (Vendor Risk)	Establish formal third-party risk management process, Require security questions during onboarding, Define minimum security requirements for vendors, Conduct periodic reviews of high-risk vendors	Vendor Risk Manager	Planned – vendor risk assessment process under development; security questionnaire selected.	150 Days from assessment				12	#N/A
R-06 (Sec Training)	Impliment role-based security training, Conduct periodic simulations, Track and report training completion metrics, Reinforce incident reporting procedures	Security Awareness Program Manager	Completed – role-based security awareness training delivered; phishing simulations conducted and completion tracked.	90 Days from assessment	3/31/2026	Mild	Low	10	2

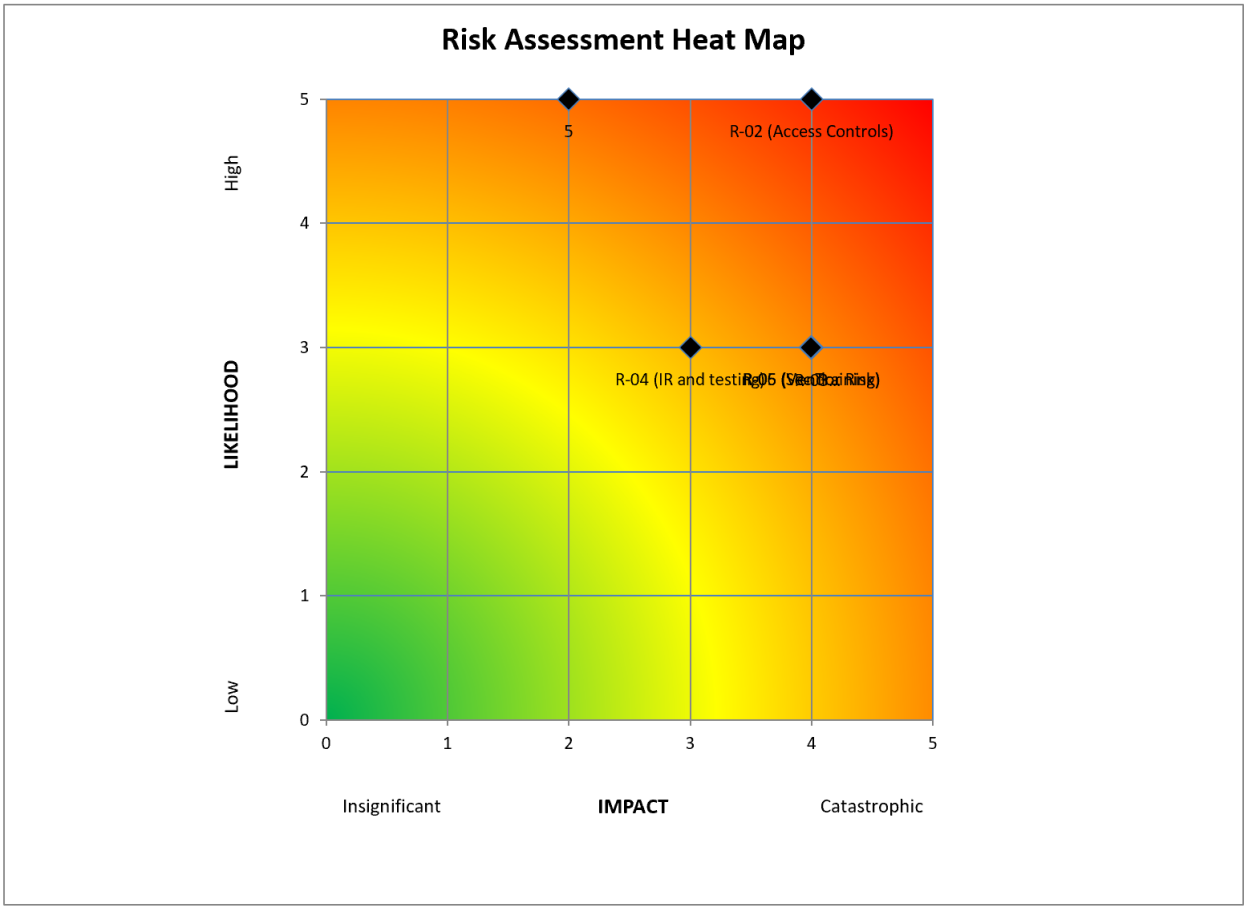
Key Observations

- All identified risks have assigned owners and defined treatment strategies.
- High and medium level risks are tracked with target completion dates and status updates.
- Residual risk scores reflect projected risk reduction following planned remediation activities.

The risk register is reviewed and updated on a recurring basis as part of ongoing risk management activities.

Heat Map Overview

The risk heat map provides a visual representation of the organization's risk landscape based on inherent risk scores derived from the risk register. Risks plotted in the red zone represent higher exposure and require prioritized attention, while yellow and green zones indicate moderate and lower levels of inherent risk, respectively. The heat map reflects the organization's current risk profile prior to the application of additional mitigation measures. This visualization enables leadership to quickly identify areas of elevated exposure and focus risk management discussions accordingly. The heat map serves as a decision-support tool for prioritizing risks based on their potential business impact and likelihood.



How to Understand:

- Y-axis: Likelihood (Low to High)
- X-axis: Impact (Low to High)
- Color Coding:
  - ❖ Red = High Risk
  - ❖ Yellow = Medium Risk
  - ❖ Green = Low Risk

Key Observations:

- Most identified risks fall within the medium to high inherent risk range based on current conditions.
- Elevated inherent risk is observed in areas such as phishing, access control, incident response, and third-party oversight.
- Several risks appear in higher exposure zones, indicating areas that warrant prioritization in risk management discussions.

Gap Analysis

This gap analysis evaluates the organization's current security posture against selected control expectations from NIST SP 800-53 Rev. 5 to identify areas where controls are fully implemented, partially implemented, or missing.

Control Area	NIST Control Reference	Current State	Target State	Gap Identified	Gap Type	Planned Action
Security Awareness & Training	AT-2, AT-3	Annual general security training with limited effectiveness tracking	Role-based security awareness training with periodic phishing simulations and completion metrics	Training lacks role-based focus and measurable effectiveness	Process	Implement role-based training, conduct phishing simulations, and track completion and results
Access Control Governance	AC-2, AC-6, IA-2	Access granted on request with informal role alignment and limited review	Documented role-based access control with regular access reviews and approval tracking	No formal access review process or documented role definitions	Governance	Establish quarterly access reviews and formalize role-based access definitions
Logging & Monitoring	AU-2, AU-6	Logs enabled on systems with limited centralized review	Centralized log aggregation with defined alerting and review procedures	Lack of centralized monitoring and regular log review	Technology	Implement SIEM or centralized logging solution with alerting for high-risk events
Incident Response Planning & Testing	IR-1, IR-4, IR-8	Incident response plan exists in draft form with ad hoc execution	Formally approved, documented, and tested incident response plan	Incident response plan not formally approved or tested	Governance	Finalize and approve IR plan; conduct annual tabletop exercises and document lessons learned
Third-Party / Vendor Risk Management	SA-9, RA-3	Vendors onboarded based on business need with basic contractual protections	Formal vendor risk assessment and ongoing monitoring program	No standardized vendor risk assessment or reassessment process	Process	Implement vendor security questionnaires and periodic reviews of high-risk vendors
Privileged Access Oversight	AC-5, AC-6	Privileged accounts exist with limited tracking and oversight	Clearly identified, documented, and monitored privileged access	Privileged access not consistently identified or reviewed	Governance	Identify privileged accounts and enforce approval, tracking, and review requirements

Summary

The gap analysis identified several areas where existing controls are partially implemented or informal when measured against NIST SP 800-53 Rev. 5 expectations. The most significant gaps were observed in access control governance, centralized logging and monitoring, incident response testing, and third-party risk oversight. While baseline controls exist in most areas, gaps are primarily related to documentation, consistency, and formalization rather than complete absence of controls. Planned remediation actions are aligned with the identified gaps and are tracked through the risk register to ensure accountability. Addressing these gaps will improve control maturity and support ongoing compliance and risk management objectives.

Treatment Options & Recommendations

Following the completion of the enterprise risk assessment, AtlasPay developed and initiated targeted risk treatment actions to address identified information security and operational risks. Treatment strategies were selected based on inherent risk severity, business impact, and feasibility of remediation, with a primary focus on mitigating risks through strengthened controls, improved governance, and enhanced oversight. Each risk was assigned a responsible owner, defined remediation actions, and a target completion timeline to ensure accountability and progress tracking. The following summary outlines the actions taken and planned to manage the organization's most significant risks.

R-01: Phishing Attacks

Phishing was identified as a high-priority risk due to its likelihood and potential impact on financial systems and sensitive data. To address this risk, AtlasPay implemented multi-factor authentication for all finance and privileged user accounts and deployed phishing simulation exercises to improve employee awareness and response. These actions were completed within the defined remediation window and are supported by ongoing monitoring of authentication and user activity. As a result, the likelihood of successful phishing attacks has been significantly reduced, lowering the overall residual risk while maintaining awareness of the persistent threat landscape.

R-02: Access Control Weaknesses

Access control deficiencies were identified as a key risk due to inconsistent enforcement of least privilege and limited documentation of access approvals. In response, AtlasPay initiated the development of a formal access review process, including the establishment of role-based access definitions and documented approval requirements for privileged access. While these actions are currently in progress, ownership has been assigned and implementation milestones have been defined. Completion of these efforts is expected to improve governance, reduce unauthorized access risk, and support compliance with access management best practices.

R-03: Logging and Monitoring Gaps

Insufficient centralized logging and monitoring capabilities were identified as a medium inherent risk due to their impact on incident detection and response. To address this risk, AtlasPay has planned the implementation of centralized log aggregation and enhanced alerting for high-risk events. Evaluation of logging and SIEM solutions is currently underway, with requirements being defined to ensure adequate coverage and monitoring effectiveness. These actions are intended to strengthen detective controls and improve visibility into system activity once implemented.

R-04: Incident Response Planning and Testing

The assessment identified gaps in incident response readiness related to documentation, approval, and testing of response procedures. Planned treatment actions include finalizing and formally approving the incident response plan, defining escalation paths, and conducting

tabletop exercises to validate response effectiveness. These activities are scheduled and pending executive approval. Once completed, they are expected to improve preparedness, coordination, and recovery capabilities in the event of a security incident.

R-05: Third-Party and Vendor Risk Management

Vendor risk was identified as a notable exposure due to the lack of a formal third-party risk assessment and monitoring process. To mitigate this risk, AtlasPay has initiated the development of a structured vendor risk management program, including the selection of security questionnaires and the definition of minimum security requirements for vendors. Periodic reviews of high-risk vendors are planned as part of ongoing oversight. These actions aim to reduce exposure introduced by third parties and improve compliance and data protection assurances.

R-06: Security Awareness and Training

Security awareness and training were identified as an area requiring improvement due to reliance on generalized training and limited effectiveness measurement. In response, AtlasPay implemented role-based security awareness training and conducted phishing simulations to reinforce user vigilance. These actions have been completed and are supported by tracked training completion metrics. Strengthening security awareness is expected to reduce the likelihood of user-driven security incidents and support the effectiveness of other preventive controls.

Conclusion

The risk treatment actions outlined above demonstrate AtlasPay's commitment to addressing identified risks through structured remediation, defined ownership, and measurable outcomes. While several risks have already been mitigated through completed actions, others remain in progress and will continue to be monitored through the risk register. This approach enables leadership to track remediation status, prioritize remaining efforts, and reassess risk as controls mature. Overall, the organization's risk posture is improving, with continued focus required to complete planned actions and sustain long-term risk management effectiveness.

***Progress against these treatment actions will be reviewed on a recurring basis and incorporated into future risk assessments and reporting cycles. ***

Documentation Overview

This documentation package supports the organization's risk management activities by capturing assessment results, decision-making rationale, and remediation tracking in a consistent and repeatable manner. The materials included provide traceability from identified risks through treatment actions, ownership, and review timelines. Documentation aligns with NIST SP 800-53 Rev. 5 and the NIST Cybersecurity Framework to support governance, compliance, and audit readiness. All artifacts are intended to be maintained as living documents and updated as risks, controls, and business conditions evolve. This approach ensures transparency, accountability, and continuity in risk management practices.

Document	Description	Owner	Review Frequency
Risk Assessment	Identifies and evaluates inherent risks	Risk Management	Annually
Risk Register	Tracks risks, ownership, and status	Risk Management	Quarterly
Risk Heat Map	Visualizes inherent risk prioritization	Risk Management	Quarterly
Risk Treatment Plan	Documents remediation actions	Control Owners	As needed
Gap Analysis	Identifies control gaps vs NIST	Risk Management	Annually
Incident Response Plan	Guides incident handling	IT Security	Annually
Security Awareness Materials	Training and simulations	HR / IT Security	Annually

Governance & Maintenance Statement

Ownership for each document is defined to ensure accountability for accuracy, updates, and ongoing relevance. Risk-related documentation is reviewed on a recurring basis and updated following significant changes to the threat landscape, business operations, or regulatory requirements. Findings from reviews and assessments are incorporated into subsequent risk management cycles to support continuous improvement. This governance approach helps ensure that documentation remains current, reliable, and actionable.