CREATED BY: IFEANYI IJEZIE

FEBRUARY 6. 2026

ATLASPAY

Enterprise Cyber Risk Profile

EXECUTIVE RISK OVERVIEW AND GOVERNANCE SUMMARY

HTTPS://WWW.LINKEDIN.COM/IN/IFEANYI-IJEZIE/

IFEANYIRMF@YAHOO.COM

EXECUTIVE SUMMARY

AtlasPay operates as a payment processing organization that depends on the continuous availability, integrity, and confidentiality of financial and customer data. As a result, cyber risk represents a direct business risk with potential financial, operational, regulatory, and reputational consequences. Disruptions such as unauthorized access, third-party breaches, or prolonged service outages have the potential to materially impact revenue, customer trust, and regulatory standing.

This Enterprise Cyber Risk Profile provides executive leadership with a consolidated view of AtlasPay's cybersecurity risk posture, key risk drivers, and governance structure. It synthesizes findings from formal risk assessments, scenario-based analyses, policy development, and business continuity planning into a single, decision-support document. The objective is to enable leadership to understand which risks matter most, why they matter, and how they are being managed.

The risk profile demonstrates that AtlasPay has identified its highest-impact risks, aligned controls and policies to those risks, and established governance mechanisms to monitor and respond to evolving threats. While the organization's overall risk posture is manageable, targeted improvements are required in access governance, third-party oversight, incident readiness, and operational resilience to reduce the likelihood and impact of high-risk scenarios.

1. ORGANIZATIONAL & OPERATING CONTEXT

1.1 BUSINESS MODEL OVERVIEW

AtlasPay provides payment processing services that handle sensitive financial transactions and customer data. Core business operations depend on uninterrupted transaction processing, secure access to systems, and trusted integrations with banking partners and third-party service providers. Because revenue generation is directly tied to system availability and transaction integrity, even short disruptions can result in financial loss, customer dissatisfaction, and regulatory scrutiny.

Cybersecurity risk therefore extends beyond technical concerns and directly affects AtlasPay's ability to meet contractual obligations, maintain regulatory compliance, and preserve its reputation as a reliable financial services provider.

1.2 TECHNOLOGY & DEPENDENCY LANDSCAPE

AtlasPay's operational environment relies on a combination of internal systems and external dependencies, including cloud-hosted infrastructure, identity and access management platforms, payment gateways, banking partners, and third-party service providers. Key personnel across Information Security, Operations, Finance, and Vendor Management play a critical role in maintaining these services.

This dependency model introduces concentration risk, particularly where third-party outages, access control failures, or monitoring gaps could disrupt core payment operations or delay incident detection and response.

2. RISK GOVERNANCE & APPETITE

2.1 RISK APPETITE STATEMENT

AtlasPay maintains a low tolerance for risks that could materially disrupt payment processing, expose sensitive financial or customer data, or result in regulatory violations. The organization has a moderate tolerance for short-term internal disruptions that do not directly impact customers or financial integrity. There is minimal tolerance for risks that undermine customer trust, contractual obligations, or regulatory compliance.

Risk treatment decisions prioritize protecting revenue, maintaining service availability, and meeting regulatory expectations over rapid restoration when tradeoffs are required.

2.2 RISK MANAGEMENT STRUCTURE

Cyber risk management at AtlasPay is conducted through a structured program that includes periodic risk assessments, scenario-based analysis, documented policies, and executive escalation procedures. Identified risks are documented in a centralized risk register with defined ownership, impact and likelihood scoring, and remediation tracking. Policies and continuity plans serve as governance mechanisms to enforce controls and guide response during disruptive events.

3. RISK IDENTIFICATION & ASSESSMENT METHODOLOGY

3.1 ASSESSMENT APPROACH

AtlasPay's risk assessments are conducted using a methodology aligned with NIST SP 800-53 Rev. 5 and informed by the NIST Cybersecurity Framework. Risks are identified through analysis of threats, vulnerabilities, and potential business impact. Both inherent and residual risk are evaluated using a quantitative impact and likelihood scoring model to ensure consistency and repeatability.

Scenario-based analyses are used to validate risk assumptions and assess how realistic threat events could affect operations, data, and regulatory obligations.

3.2 IMPACT & LIKELIHOOD SCALES

Risk impact is evaluated across four categories: financial, operational, regulatory, and reputational. Likelihood reflects the probability of occurrence based on threat prevalence, control maturity, and environmental factors. Combined impact and likelihood scores determine overall inherent and residual risk ratings.

What is the risk?	Risk Category	Existing Controls	Comments/Concerns	Impact(Inherent)	Likelihood(Inherent)	Risk Calculation		
						Impact	Likelihood	Risk Score
R-01 (Phishing attacks)	Operational	Email filtering, annual 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	Significant	High	4	5	20
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
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
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
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	Significant	Medium	4	3	12
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

4. ENTERPRISE RISK LANDSCAPE

4.1 KEY RISK THEMES

Analysis of AtlasPay's environment identified five primary cyber risk themes:

- **Access and Privileged Account Risk:** Unauthorized or excessive access could enable fraud, data exposure, or system manipulation with severe financial and regulatory consequences.
- **Third-Party and Vendor Risk:** Dependence on external service providers introduces exposure outside of direct organizational control.
- **Incident Response Readiness:** Gaps in formalized response procedures and testing increase the potential impact of security incidents.
- **Operational Resilience and Availability:** System outages or service disruptions directly affect revenue and customer trust.
- **Human and Awareness Risk:** User behavior remains a contributing factor in phishing, credential compromise, and security incidents.

Each theme maps directly to risks documented in the enterprise risk register and validated through scenario analysis.

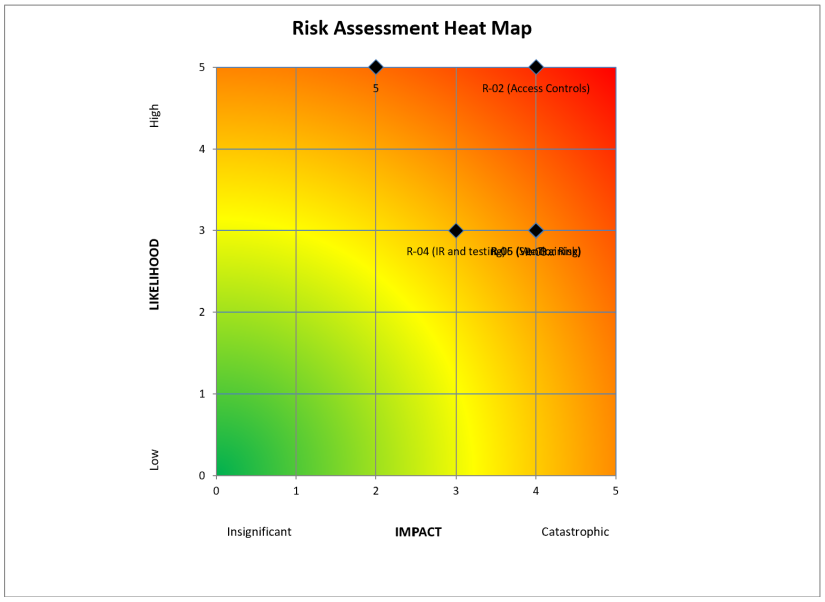
4.2 RISK REGISTER SUMMARY

The enterprise risk register consolidates all identified risks into a structured management view. Each risk includes defined ownership, inherent and residual risk ratings, selected treatment strategies, and remediation timelines. High and medium risks are actively tracked to ensure accountability and progress.

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

4.3 RISK HEAT MAPS OVERVIEW

The risk heat map provides a visual representation of AtlasPay's inherent risk landscape prior to mitigation. Risks in the red zone represent the highest exposure and require prioritized attention. Yellow and green zones reflect moderate and lower exposure levels.



This visualization supports executive decision-making by highlighting which risks pose the greatest potential impact on business operations and financial stability.

5. SCENARIO-BASED RISK VALIDATION

5.1 PRIVILEGED ACCOUNT ABUSE

The privileged account abuse scenario demonstrated how misuse or compromise of elevated access could result in catastrophic impact due to unauthorized transactions, data manipulation,

and regulatory exposure. Inherent risk was assessed as high to catastrophic, driven by severe impact and moderate likelihood. This scenario validates access control governance as a top risk priority.

5.2 THIRD-PARTY VENDOR BREACH SCENARIO

The third-party vendor breach scenario highlighted the risk introduced by external providers with access to sensitive systems or data. A breach at a trusted vendor could result in data exposure, regulatory penalties, and operational disruption. Inherent risk was assessed as catastrophic, reinforcing the need for formal vendor risk management and continuous oversight.

6. RISK TREATMENT & CONTROL ALIGNMENT

6.1 POLICY-TO-RISK MAPPING

AtlasPay has implemented targeted policies to address identified risk themes:

- **Access Control & Privileged Access Policy:** Mitigates access abuse and least privilege risks
- **Third-Party Risk Management Policy:** Addresses vendor and outsourcing risk
- **Incident Response Policy:** Supports detection, escalation, and coordinated response
- **Security Awareness & Acceptable Use Policy:** Reduces human-driven risk
- **Business Continuity Plan:** Supports operational resilience during major disruptions

RISK ID	RISK DESCRIPTION	PRIMARY IMPACT	MITIGATING POLICY / DOCUMENT
R-01	PHISHING AND CREDENTIAL COMPROMISE	FINANCIAL, OPERATIONAL, REPUTATIONAL	SECURITY AWARENESS & ACCEPTABLE USE POLICY
R-02	PRIVILEGED ACCESS MISUSE OR ABUSE	FINANCIAL, REGULATORY	ACCESS CONTROL & PRIVILEGED ACCESS POLICY
R-03	THIRD-PARTY VENDOR SECURITY BREACH	REGULATORY, REPUTATIONAL	THIRD-PARTY RISK MANAGEMENT POLICY
R-04	DELAYED OR INEFFECTIVE INCIDENT RESPONSE	OPERATIONAL, REGULATORY	INCIDENT RESPONSE POLICY
R-05	PROLONGED SERVICE OUTAGE OR DISRUPTION	FINANCIAL, OPERATIONAL	BUSINESS CONTINUITY PLAN
R-06	INADEQUATE USER SECURITY AWARENESS	OPERATIONAL, REPUTATIONAL	SECURITY AWARENESS & ACCEPTABLE USE POLICY

6.2 RISK TREATMENT STRATEGY

Most identified risks are addressed through mitigation strategies focused on strengthening preventive and detective controls. Residual risk is accepted where further reduction would be disproportionate to business benefit. Risk ownership and remediation tracking are managed through the enterprise risk register.

7. BUSINESS CONTINUITY & RESILENCE INTEGRATION

7.1 CONTINUITY TRIGGERS AND ESCALATION

Business continuity planning is aligned with identified risk scenarios and impact thresholds. Activation criteria include payment processing outages, cyber incidents requiring system shutdown, prolonged third-party outages, or executive determination that continuity actions are required.

7.2 BUSINESS IMPACT ANALYSIS ALIGNMENT

The Business Impact Analysis (BIA) defines recovery priorities using RTO and RPO values that align directly with risk impact scoring. Critical services such as payment processing and fraud monitoring receive the highest recovery priority, ensuring continuity strategies reflect business risk realities.

Business Function	Maximum Tolerable Downtime	RTO	RPO	Key Dependencies
Payment Processing	24 hours	4 hours	Near-real-time	Cloud provider, payment gateway
Customer Account Access	48 hours	8 hours	24 hours	Identity provider, application platform
Fraud Monitoring	24 hours	4 hours	Near-real-time	Monitoring tools, transaction data
Financial Reporting	72 hours	24 hours	24 hours	Finance systems, data warehouse

8. RESIDUAL RISK & MATURITY OUTLOOK

While AtlasPay has established a solid foundation for cyber risk governance, residual risk remains due to evolving threats, third-party dependencies, and operational complexity. Continued improvement opportunities include enhanced monitoring, recurring testing of response and continuity plans, and increased measurement of control effectiveness through metrics and key risk indicators.

9. FRAMEWORK ALIGNMENT & GOVERNANCE REFERENCE

This risk profile and supporting artifacts are informed by recognized industry frameworks, including:

- NIST Cybersecurity Framework
- NIST SP 800-53 Rev. 5

These frameworks guide structure and governance but are applied in a risk-based, business-focused manner rather than as checklist compliance exercises.

CONCLUSION

This Enterprise Cyber Risk Profile provides AtlasPay with a consolidated, executive-level view of cybersecurity risk and governance. By aligning risk assessment, scenario analysis, policy development, and business continuity planning, AtlasPay demonstrates a mature and intentional approach to managing cyber risk. The organization is well-positioned to reduce high-risk exposures, support informed decision-making, and strengthen long-term operational resilience as the threat landscape evolves.