ATLASPAY

Business Continuity Plan

By: Ifeanyi Ijezie

https://www.linkedin.com/in/ifeanyi-ijezie/

TABLE OF CONTENTS

Version: 1.0

Effective Date: ____________________

BCP Owner: ____________________

Review Frequency: Annual

Classification: Internal

1. EXECUTIVE SUMMARY

This Business Continuity Plan defines how AtlasPay will maintain or restore critical business operations during and after disruptive events that materially impact normal operations. As a payment processing organization handling sensitive financial and customer data, AtlasPay faces operational, financial, and regulatory risk from events such as cyber incidents, third-party outages, and technology failures.

Given AtlasPay's resilience on continuous transaction processing and third-party integrations, extended service disruption presents immediate financial and customer trust. The purpose of this plan is to minimize financial loss, service disruption, and reputational damage by prioritizing critical services, establishing recovery objectives, and defining escalation and communication processes. This plan supports executive decision-making by clearly outlining when continuity actions are required and how recovery efforts are coordinated. The BCP is designed to function alongside incident response and disaster recovery activities as part of AtlasPay's broader risk management program.

2. PURPOSE AND OBJECTIVES

2.1 Purpose

The purpose of this Business Continuity Plan is to establish a structured approach for maintaining or restoring AtlasPay's critical business functions during disruptive events that cannot be resolved through normal operating procedures.

2.2 Objectives

The objectives of this plan are to:

- *Reduce downtime of critical payment and financial operations.*
- *Protect revenue, customer trust, and regulatory standing.*
- *Support timely and informed executive decision-making.*
- *Ensure coordinated response across business, technology, and vendor teams.*
- *Enable predictable and prioritized recovery of critical services.*

3. SCOPE AND ASSUMPTIONS

3.1 Scope

This plan applies to business processes, systems, personnel, and third-party dependencies that support AtlasPay's core payment processing and financial operations. It includes disruptions caused by cyber incidents, technology outages, third-party failures, and other events that materially impact service availability.

3.2 Assumptions

- *Not all disruptions can be prevented, but their impact can be managed*
- *Some services may operate at reduced capacity during recovery*
- *Third-party vendors play a critical role in continuity*
- *Executive leadership is available to make continuity decisions during major disruptions*

3.3 Out of Scope

This plan does not provide detailed technical recovery procedures or system-level restoration steps, which are addressed in separate incident response and disaster recovery documentation.

4. BUSINESS CONTEXT

4.1 Critical Services

AtlasPay's most critical services include:

- *Payment transaction processing and settlement*
- *Customer access to payment and account services*
- *Fraud monitoring and transaction integrity controls*
- *Financial reporting and reconciliation activities*
- *Third-party integrations supporting payment operations*

4.2 Key Dependencies

Critical dependencies include:

- *Cloud hosting and identity management providers*
- *Payment gateways and banking partners*
- *Third-party service providers supporting monitoring and customer operations*
- *Secure network connectivity and remote access*
- *Key personnel within IT, Security, Finance, and Vendor Management*

5. BUSINESS IMPACT ANALYSIS SUMMARY

The Business Impact Analysis identifies and prioritizes functions based on their tolerance for disruption.

5.1 Impact Categories

Disruptions are evaluated based on:

- *Financial impact (lost revenue, penalties, remediation costs)*
- *Operational impact (service downtime, processing delays)*
- *Regulatory impact (compliance violations, reporting obligations)*
- *Reputational impact (customer trust and market confidence)*

5.2 Critical Functions and Prioritization Table

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

This prioritization guides recovery sequencing and resource allocation.

6. CONTINUITY STRATEGIES

6.1 People Workarounds

- *Cross-training and role coverage for critical functions*

- *Defined escalation paths for decision authority*
- *Remote work enablement for continuity scenarios*

6.2 Alternative Processes

- *Manual approval or processing workarounds where feasible*
- *Prioritization of high-impact customer transactions*
- *Temporary suspension of non-critical activities*

6.3 Technology Alternatives

- *Use of redundant systems and backups where available*
- *Controlled restoration of services based on priority*
- *Coordination with disaster recovery procedures*

6.4 Third-Party/Vendors

- *Engagement of vendors during outages*
- *Use of contractual escalation and notification requirements*
- *Assessment of alternate service options where feasible*

7. INCIDENT RESPONSE VS BUSINESS CONTINUITY

Incident Response focuses on identifying, containing, and resolving security or operational incidents. Business Continuity is activated when the disruption significantly impacts AtlasPay's ability to operate critical business functions beyond normal response capabilities. Disaster Recovery supports the technical restoration of systems. These activities operate in coordination but serve distinct purposes.

8. PLAN ACTIVATION AND ESCALATION

8.1 Activation Criteria

This plan may be activated when:

- *Payment processing is unavailable or severely degraded*
- *A cyber incident requires system shutdown*
- *A critical third-party vendor experiences a prolonged outage*
- *Executive leadership determines continuity actions are required*

8.2 Severity Levels (Low/Med/High)

Severity levels are used to assess the potential business impact and urgency of a disruption. Low severity events have minimal operational impact and can be managed through standard incident response processes. Medium severity events result in partial service degradation or elevated risk and may require increased coordination. High severity events materially impact critical services, customer operations, or regulatory obligations and may warrant activation of this Business Continuity Plan.

Severity Level	Description	Typical Response
Low	Minimal operational impact; no customer-facing disruption	Managed through standard incident response
Medium	Partial service degradation or elevated operational risk	Increased coordination and leadership awareness
High	Material impact to critical services, customers, or regulatory obligations	Executive involvement and potential BCP activation

8.3 Escalation Path and Decision Authority

Role	Escalation Responsibility
Information Security	Identify incident, assess impact, recommend escalation
Operations	Assess service impact and operational disruption
Executive Sponsor	Authorize BCP activation and continuity actions
Legal / Compliance	Advise on regulatory and contractual obligations
Communications	Coordinate internal and external messaging

Escalation decisions prioritize maintaining customer trust and regulatory compliance over rapid restoration when tradeoffs are required.

9. COMMUNICATIONS PLAN

9.1 Internal Communications

- *Executive and leadership briefings*
- *Employee status updates as appropriate*

9.2 Customer Communications

- *Timely, coordinated messaging for service disruptions*
- *Clear guidance on service availability and expectations*

9.3 Regulatory/Legal Notifications

- *Notifications coordinated with Legal and Compliance*
- *Adherence to applicable reporting obligations*

9.4 Vendor Communications

- *Engagement with impacted vendors*
- *Status updates and recovery coordination*

10. RECOVERY PROCEDURES

- ***Payment Processing Disruption:*** *Prioritize transaction integrity and controlled service restoration*
- ***Third-Party Vendor Outage:*** *Engage vendor escalation and assess alternate workflows*
- ***Cyber Incident Shutdown:*** *Coordinate IR, DR, and continuity actions*
- ***Loss of Key Personnel****: Activate role coverage and leadership escalation*

11. TESTING AND MAINTENANCE

- *Tabletop exercises conducted at least annually*
- *Updates based on lessons learned and environmental changes*
- *Documentation of test results and improvement actions*

12. FRAMEWORK ALIGNMENT

This business continuity plan is informed by industry recognized risk management and resilience frameworks, including NIST SP 800-53 Rev. 5 (Contingency Planning and Incident Response), NIST Cybersecurity Framework, and ISO/IEC 27001 business continuity principles. These frameworks were used to support governance alignment, audit readiness, and consistent risk management practices, rather than to prescribe control-level implementation. The plan is designed to integrate with AtlasPay’s broader risk management, incident response, and third-party risk programs.

13. ROLES AND RESPONSIBILITIES

- ***Executive Sponsor:*** *Provides strategic direction and decision authority*
- ***BCP Owner:*** *Maintains the plan and coordinates continuity activities*
- ***Information Security:*** *Supports incident coordination and risk assessment*
- ***Operations:*** *Executes continuity strategies*
- ***Legal and Compliance:*** *Advises on regulatory obligations*
- ***Vendor Management:*** *Coordinates third-party continuity efforts*

CONCLUSION

This Business Continuity Plan provides AtlasPay with a structured, risk-based approach to maintaining critical operations during disruptive events. By prioritizing essential services, defining recovery objectives, and establishing clear governance, AtlasPay strengthens its operational resilience and ability to protect revenue, customers, and regulatory standing. The plan is intended to evolve as the organization grows and as risks, dependencies, and business conditions change.

APPENDIX A: CONTACT LIST

This appendix identifies key personnel and escalation contacts required to support business continuity and recovery activities. Contact information must be kept current to ensure timely communication during disruptive events.

Role	Name / Title	Primary Contact	Secondary Contact
Executive Sponsor			
BCP Owner			
Information Security Lead			
Operations Lead			
Legal / Compliance			
Vendor Management			
Communications / PR			

(This contact list shall be reviewed and updated at least annually or upon personnel changes to ensure accuracy during continuity events).

APPENDIX B: CRITICAL VENDOR LIST

Vendor Category	Vendor Name	Service Provided	Criticality	Primary Contact	Escalation Path
Cloud Hosting	__________	IaaS	High	__________	__________
Payment Gateway	__________	Payment Processing	High	__________	__________
Banking Partner	__________	Settlement / Clearing	High	__________	__________
Identity Provider	__________	Authentication / Access	Medium	__________	__________
Monitoring / SIEM	__________	Logging & Monitoring	Medium	__________	__________

GLOSSARY

BCP (Business Continuity Plan)

A documented strategy outlining how an organization will maintain or restore critical business operations during and after a disruptive event.

BIA (Business Impact Analysis)

A structured analysis used to identify critical business functions and assess the impact of disruptions over time, supporting prioritization and recovery planning.

MTD (Maximum Tolerable Downtime)

The maximum length of time a business function can be unavailable before causing unacceptable operational, financial, or regulatory impact.

RTO (Recovery Time Objective)

The targeted duration of time within which a business function or system must be restored following a disruption.

RPO (Recovery Point Objective)

The maximum acceptable amount of data loss measured in time, indicating how far back data restoration must recover.

IR (Incident Response)

The coordinated activities used to identify, contain, investigate, and remediate security or operational incidents.

DR (Disaster Recovery)

The technical process of restoring IT systems, infrastructure, and applications following a major outage or failure.

SIEM (Security Information and Event Management)

A technology solution used to collect, analyze, and correlate security logs and events for monitoring, detection, and response.

IaaS (Infrastructure as a Service)

A cloud computing model that provides virtualized computing resources such as servers, storage, and networking.

PR (Public Relations)

The function responsible for managing external communications and public messaging during significant events.

Executive Sponsor

A senior leader with decision-making authority responsible for strategic oversight and activation of continuity actions.

Critical Function

A business process or service essential to revenue generation, customer service, regulatory compliance, or organizational survival.

Third-Party Vendor

An external organization that provides services, systems, or support to AtlasPay and may introduce operational or security risk.

Continuity Event

Any disruption that materially impacts normal operations and requires activation of business continuity strategies beyond routine incident handling.