



Business Continuity Executive Overview

Operational Resilience & Recovery Commitments — Version 1.0 · 2026

Document	Business Continuity Executive Overview
Audience	Clients, prospects and partners
Owner	Chief Operations Officer (COO)
Review frequency	At least annually
Effective date	April 2026
Contact	security@wiseathena.com

1. Purpose & Commitment

WiseAthena is committed to maintaining operational continuity in the face of unplanned disruptions. Our Business Continuity Programme ensures that we can maintain or rapidly restore the services our clients depend on, regardless of the nature or cause of any interruption.

This document provides a public overview of our Business Continuity Programme for the benefit of clients and partners who wish to understand our resilience posture. The full Business Continuity Policy and supporting plans are internal documents subject to information security controls.

2. Scope

The Business Continuity Programme covers all critical operational processes and applies to all employees, contractors and third-party providers that form part of WiseAthena's service delivery chain. It encompasses:

- All IT systems, infrastructure and cloud services supporting client service delivery
- Operational and communication processes required to maintain service continuity
- Vendor and supply chain dependencies critical to the delivery of contracted services
- All production, staging and development environments, whether local or cloud-hosted

3. Recovery Objectives

WiseAthena has defined recovery time and recovery point objectives for its critical processes. The headline objectives for client-facing services are:

PROCESS	RECOVERY TIME OBJECTIVE (RTO)	RECOVERY POINT OBJECTIVE (RPO)
Service delivery to clients	8 hours	< 1 hour

PROCESS	RECOVERY TIME OBJECTIVE (RTO)	RECOVERY POINT OBJECTIVE (RPO)
Client incident communication	First notification < 1 hour from activation	—
Client support & response	4 hours	—
Identity & access management	1 hour (urgent off-boarding)	—
Data processing & ML pipeline	8 hours	Last checkpoint
Billing & payments	24 hours	—

4. Programme Structure

Governance

The Business Continuity Programme is owned by the Chief Operations Officer (COO) and is subject to oversight by the Board of Directors and Risk Committee. Activation authority and final decision-making during an incident rests with the designated Continuity Director (COO).

A defined chain of command, with named primary and alternate roles, ensures the programme can operate without dependency on any single individual.

Plan Activation

The Business Continuity Plan is activated when a critical process exceeds its defined recovery time objective, when a major security incident is declared, or when a critical vendor failure occurs. Activation triggers an immediate, parallel response across technical recovery and client communication tracks.

Client Communication

WiseAthena is committed to proactive and timely communication with affected clients during any incident. Our standard is:

- First notification to affected clients within 1 hour of plan activation
- Regular status updates until the incident is resolved
- A post-incident summary upon closure

Client communication is managed by a dedicated point of contact and operates independently of internal technical systems.

Technical Resilience

WiseAthena's infrastructure is designed for resilience. Technical continuity measures include regional failover capability, regular data backups with defined recovery objectives, and a documented Disaster Recovery Plan complementing the Business Continuity Policy.

Workforce Continuity

The organisation operates on a fully remote model. All personnel are equipped with secure remote access capabilities and backup connectivity options. Critical roles have defined alternates with pre-configured access and documented handover materials, enabling effective continuity without dependency on any individual.

5. Testing & Continuous Improvement

The Business Continuity Programme is tested at least annually. Annual exercises include:

- Regional failover test — simulating a cloud region outage
- Backup restoration test — validating recovery of critical data
- Incident communication drill — simulating client notification procedures
- Tabletop exercise — scenario-based walkthrough of a BCP activation with all critical roles

Each exercise produces a documented record of outcomes and a Corrective Action Plan (CAPA) to address any identified gaps. Results are reviewed by the COO and Risk Committee.

The Business Continuity Policy and associated plans are reviewed at least annually, and following any significant incident, structural change or change in the organisation's risk environment.

6. Business Impact Summary

The organisation has performed a formal Business Impact Analysis (BIA) identifying critical processes, their dependencies and the potential impact of prolonged interruption. Impact categories assessed include:

- **Financial impact** — SLA penalties, emergency recovery costs, potential client churn
- **Reputational impact** — client-visible outages and data security events
- **Regulatory impact** — notification obligations arising from incidents involving personal data
- **Operational impact** — loss of monitoring, deployment capability or key personnel

The BIA informs the prioritisation of recovery efforts and the investment in preventive controls.

7. Contact

For questions about WiseAthena's Business Continuity Programme, or to discuss resilience requirements as part of a commercial or procurement process, please contact:

Business continuity enquiries

security@wiseathena.com

Exceptions to security policies require formal documentation and approval in accordance with the organisation's Policy Management Procedures.