ApertureRisks
SEE RISK. PRIORITIZE. TAKE ACTION.

BUYER ASSURANCE STATEMENT

Operating Assurance and Business Continuity Statement

A candid buyer-assurance summary of current support capacity, escalation targets, infrastructure boundaries, continuity limitations, and Client exit rights.

OPERATOR

PWLogiConGroup LLC, operator of the ApertureRisks platform

Document version: 1.0 - July 19, 2026

Procurement review copy | aperturerisks.com | ian@pwlogicongroup.com

Purpose

This statement provides a candid, procurement-ready summary of current support capacity, escalation targets, infrastructure boundaries, continuity limitations, and Client exit rights. It is not a guarantee.

1. Current operating model

Delivery is principal-led under PWLogiConGroup LLC. Named backup personnel are not currently represented as available. Uninterrupted service is not guaranteed. Buyer-specific continuity requirements must be negotiated before sensitive intake.

2. Support hours

Current support hours are U.S. business days, 9:00 a.m.-5:00 p.m. Eastern Time. No 24x7 support or availability is represented.

3. Response targets

- Critical: same business day during the current support window.
- High: one business day.
- Standard: two business days.

These are operating targets, not contractual SLAs or response guarantees. No service credits are included unless stated in an executed agreement.

4. Escalation route

Operational and security issues route to ian@pwlogicongroup.com. Tenant-isolation and material security issues are treated as Critical until triaged. No additional named technical responder is represented as available.

5. Source and deployment control

Application source and committed deployment-related files are version controlled. Runtime secrets and environment settings are managed separately in the deployment platform and are not represented as fully version controlled.

No claim is made that infrastructure provisioning is comprehensive or fully code-driven, that every deployment step is automated, or that production has no manual dependencies.

6. Documentation

Maintained materials include assessment scope documents, delivery stages, service boundaries, methodology, control summaries, exit requirements, and repository-based application documentation. Complete architecture runbooks or seamless knowledge transfer are not represented as tested capabilities.

7. Security boundaries

- Connector credential payloads use AES-256-GCM before persistence.
- Signed OAuth state is tenant- and provider-bound and expires after ten minutes.
- Authenticated workflows enforce tenant context and role permissions.
- Tenant connectors require administrator enablement and fail closed.
- Recommendations require human review.
- Email connectors create drafts and do not authorize sending.

These scoped controls do not represent AES-256-GCM for every stored record, file, log, or backup; TLS 1.3 for all transport; mandatory MFA across every provider; an independent penetration test; or an independent security audit.

8. Certification and attestation status

SOC 2 has not been completed. ISO 27001 has not been completed. FedRAMP authorization has not been completed. No active audit or certification is claimed. No independent penetration test or third-party security attestation is claimed. Future attestations will be evaluated against customer and contractual requirements.

No readiness program, active alignment, target audit quarter, or readiness-complete status is represented.

9. Hosting and resilience

Hosting and provider-specific architecture details are confirmed during qualified security review where appropriate. No multi-region deployment, multi-zone redundancy, automated failover, or tested disaster-recovery capability is claimed.

10. Recovery boundaries

No independently validated disaster-recovery capability is claimed. No contractual RTO or RPO exists by default. Backup, recovery, escrow, alternate staffing, and continuity requirements require written agreement.

No recovery time, recovery point, backup schedule, or tested restoration result is represented unless documented and agreed.

11. Client data rights

Export, return, retention, and deletion requirements are agreed by engagement. Client-specific rights and timelines must be documented in the SOW or order form. Legal, backup, archival, and provider-retention exceptions must be identified.

No immediate deletion from every system, cryptographic deletion from every system, deletion from backups on demand, or guaranteed Certificate of Deletion is represented.

12. Closing boundary

This document is a buyer-assurance summary. It is not an independent audit, certification, penetration test, uptime commitment, SLA, disaster-recovery guarantee, or substitute for a signed agreement.