Risk Studio

SECURITY AND DATA RESIDENCY

A clear boundary for sensitive client data.

A concise procurement briefing on identity, isolation, client-controlled storage, safe audit metadata, support and the limits of the hosted candidate.

Controlled availability. Risk Studio V2.12.1 is not generally available or authorised for independent client reliance. The client's approved external engine remains the formal system of record; internal quantitative results are cross-check evidence only. QCRA is supervised-pilot only. QSCRA is not offered.

V2.12.1 | 12 July 2026 | 6 pages
Visit somariskstudio.com | Email hello@somariskstudio.com

ARCHITECTURE

The control plane coordinates. The client controls content.

This is the defining boundary for the hosted candidate.

SOMA-hosted control plane	Client-controlled storage
Identity and tenancy	Schedules and XER files
Entitlements	Risk registers and mappings
Safe audit metadata	Model inputs
Opaque storage pointers	Reports and outputs

- Credentials remain in approved secret handling and are never embedded in storage pointers.
- Sensitive scheme content is not persisted at rest on the SOMA-hosted control plane.
- Processing is authorised in verified tenant context against the approved storage route.

DATA CLASSIFICATION

What goes where.

The launch record separates low-sensitivity coordination metadata from client-controlled scheme content.

Data class	Hosted control plane	Client-controlled storage
Identity and entitlement	Required for access and authorisation	Not the system of record
Safe audit metadata	Actor, tenant, time, outcome and opaque references	Detailed evidence where contractually required
Storage pointers	Opaque configuration references only	Credentials remain in approved secret handling
Schedules and registers	Not persisted at rest	Authoritative source and working copy
Model inputs and outputs	Not persisted at rest	Stored under client policy and retention

Public request rule. No schedules, registers, credentials, connection strings, scheme identifiers or sensitive narrative.

ACCESS CONTROL

Identity, tenant and role resolve together.

Tenant isolation is release-blocking; it is not a convenience feature.

Identity

Tokens are validated for issuer, audience, signature and time before principal creation.

Tenant context

Tenant is derived from verified identity and governed routing. User-supplied query parameters do not grant access.

Authorisation

Entitlements and roles are evaluated at control-plane chokepoints. Privileged actions require the appropriate role.

Isolation evidence

A/B positive and negative tests are required. Any cross-tenant read path is a P0 release blocker.

Current candidate. The private Azure candidate is operator-restricted. Production DNS/TLS and client sign-in are not cut over.

OPERATIONS

Durability without blurring ownership.

Storage

Client-owned location, access policy and retention remain authoritative. Durable writes use controlled atomic patterns.

Backup and recovery

The contract allocates control-plane recovery and client-content backup responsibilities.

Audit

Authentication and administrative events feed tamper-evident metadata. Sensitive source content must not enter logs.

Support

Support starts from the SRS reference, tenant and opaque evidence identifiers. Client content uses only the approved route.

Self-host option

Clients that cannot permit hosted processing use a separately governed self-host deployment. Security responsibilities, updates and evidence are agreed for that pattern; it is not described as hosted SaaS.

PROCUREMENT DECISION

Confirm the boundary against your policy.

Use these questions during qualification and record each answer in the controlled evidence pack.

- Which client-controlled backend, region, keys and retention policy are approved?
- Which identity provider, domains, roles and privileged administrators are approved?
- Which processing locations and support-access conditions are contractually permitted?
- Who owns backup, recovery, incident response and evidence retention for each plane?
- Does policy require the separately governed self-host deployment?
- Which DPA, privacy, transfer, vulnerability-disclosure and security-review decisions remain open?

Honest limits. This briefing is not an independent certification, penetration-test report or substitute for the signed contract, DPA and deployment-specific evidence.

Security and procurement questions

Request the current evidence and known-limitations pack before making a decision.

Request access | Email hello@somariskstudio.com