Risk Studio

SECURITY & DATA RESIDENCY

A clear boundary for sensitive client data.

A concise procurement briefing on identity, isolation, storage, audit metadata, support and the limits of the hosted service.

CURRENT BRIEFING

V2.12.1 | 12 July 2026 | 6 pages

soma-risk-studio-83l.pages.dev | hello@somaprojectcontrols.com

SOMA Project Controls Ltd

ARCHITECTURE

The control plane coordinates. The client controls content.

This is the defining deployment boundary for the hosted service.

SOMA-HOSTED CONTROL PLANE

Identity and coordination

- Identity and tenancy
- Entitlements
- Audit metadata
- Opaque storage pointers

No schedules, risk registers or model outputs persisted at rest.

Authorised and encrypted

CLIENT-CONTROLLED STORAGE

Scheme content and evidence

- Schedules and XER files
- Risk registers and mappings
- Model inputs
- Reports and outputs

Client-selected location, access policy and retention.

Pointers identify approved storage locations without embedding credentials. Processing is authorised in tenant context; sensitive scheme content is not persisted at rest on the SOMA-hosted plane.

DATA CLASSIFICATION

What goes where.

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

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

Public request rule: no schedules, registers, passwords, connection strings or sensitive scheme narrative. The first step collects only organisation, contact and intended outcome.

ACCESS CONTROL

Identity, tenant and role are resolved together.

Tenant isolation is a release-blocking control, not a convenience feature.

Identity

Hosted deployments use the approved identity path. Tokens are validated for issuer, audience, signature and time before principal creation.

Tenant context

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

Authorisation

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

Isolation evidence

Launch requires positive and negative access tests. Any cross-tenant read path is a P0 blocker.

Access is withheld until the required identity, storage and isolation evidence is recorded as passed.

OPERATIONS

Durability without blurring ownership.

Storage

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

Back-up and recovery

The contract identifies control-plane recovery responsibilities and the client's content-store backup responsibilities.

Audit

Authentication and administrative events feed tamper-evident audit metadata. Sensitive source content must not be written to logs.

Support

Support starts from the request reference, tenant and opaque evidence identifiers. Client content is accessed only through the approved route.

SELF-HOST OPTION

Clients that cannot permit any hosted processing use the 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 the answer in the launch evidence pack.

- Is client-controlled storage acceptable, and which backend, region, keys and retention policy apply?
- 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?

HONEST LIMITS

This briefing describes the product boundary; it is not an independent certification, penetration-test report or substitute for the signed contract, DPA and deployment-specific control evidence. Current certification status must be confirmed during procurement.

Security and procurement questions: hello@somaprojectcontrols.com