RegAlign®

Penetration Test — Scope of Work

Status: Canonical scope-of-work to send to Jersey/UK-qualified pen-test providers for fixed-price quotation. Brief once, quote three times. **Owner:** Sabrina Stewart. **Purpose:** Produce a defensible pen-test letter that every CCO / MLRO can be shown on day one of any pilot or production conversation.

1. About RegAlign

- RegAlign is a single-tenant-per-customer SaaS platform serving JFSC-regulated trust and corporate services businesses.
- Architecture: TanStack Start (React + server functions) on Cloudflare Workers, Supabase (Postgres) for data and auth, RLS for tenant isolation.
- Audience for the pen-test letter: customer CCOs / MLROs, board-level technology committees, eventual JFSC interaction.
- Current stage: pre-first-production-deployment; live preview environment exists; production-grade hardening in progress.

2. Objectives

The pen test must produce:

- 1. **An executive summary** suitable for sharing with non-technical board members and customer CCOs.
- 2. **A technical findings report** with CVSS-scored issues, evidence, and remediation guidance.
- 3. **A re-test letter** confirming remediation of any High or Critical findings.
- 4. **A clean letter** suitable for customer-facing distribution once findings are remediated.

The goal is a defensible artefact, not a checkbox. The provider should expect the report to be referenced in customer due-diligence, regulator interaction, and (eventually) investor diligence.

3. In scope

Surface	What to test
Web application (authenticated)	OWASP Top 10 (current edition), session management, authorisation/access control, business-logic flaws specific to multi-tenant compliance data
Web application (unauthenticated)	Public surface, sign-up flows, password reset, marketing routes
API / server functions	TanStack `createServerFn` endpoints, server routes under `/api/`, rate limiting, input validation
Authentication	Supabase auth integration, MFA enforcement, session handling, JWT handling
Authorisation	**Row-Level Security policies** — explicit tenant-isolation testing. Attempt cross-tenant data access via crafted requests, token manipulation, parameter tampering
Data export	Customer data export endpoints, signed-URL handling, expiry

Surface	What to test
Audit trail	Hash-chain integrity, attempts to insert/modify/delete audit entries, replay attacks
Webhooks / public API (`/api/public/*`)	Signature verification, replay protection, rate limiting
Infrastructure	Cloudflare Worker configuration, Supabase configuration review (RLS coverage, exposed endpoints, service-role key handling)

Two-user test accounts will be provided in each of three customer-tenant slices to facilitate cross-tenant testing.

4. Out of scope

- Physical security (no physical premises).
- Social engineering of the founder (single-person team — not a meaningful test).
- Denial-of-service load testing (separate engagement).
- Third-party sub-processor infrastructure (Supabase, Cloudflare — both have their own SOC 2 reports we will reference).
- Mobile application (none exists).
- AI / model security beyond input validation of any AI-assisted features.

5. Methodology requirements

- **Black-box** for unauthenticated surfaces.
- **Grey-box** for authenticated surfaces — test accounts provided, source-code access provided on request under NDA.
- **Authorisation testing must be exhaustive on the multi-tenant boundary.** This is the single most important class of finding for RegAlign's customer trust narrative.
- OWASP Testing Guide alignment expected.
- All findings reproducible with documented steps.

6. Deliverables

Deliverable	Format	Audience
Executive summary	PDF, 2–3 pages	Customer CCO, board, regulator
Technical findings report	PDF + machine-readable (JSON or CSV)	RegAlign engineering
Re-test letter on remediation	PDF, 1 page	Customer-facing
Clean letter (if applicable)	PDF, 1 page	Customer-facing, shareable

Provider retains a copy for their records per their standard practice; otherwise no third-party distribution without RegAlign written consent.

7. Timeline

- Quotation expected within 5 business days of receiving this scope.
- Test window: 5–10 business days from kick-off.

- Initial findings within 5 business days of test completion.
- Final report within 10 business days of test completion.
- Re-test (if needed) within 30 days of remediation confirmation.

8. Commercial

- Fixed-price quotation expected. Day-rate quotations will not be considered.
- Re-test cost itemised separately.
- Annual retainer pricing (year 2 onwards) optional in quotation.

Indicative budget: £4,000–8,000 all-in for initial test + executive report + one re-test. Quotations materially outside this band will be considered but require justification.

9. Provider requirements

- CREST or equivalent certification preferred.
- At least one engagement-team member with demonstrable Channel-Islands or UK financial-services pen-test experience.
- Standard professional indemnity insurance in place.
- Willing to sign RegAlign NDA before receiving any technical detail beyond this scope document.

10. Quotation request

Please respond by [date, 14 days from issue] with:

- 1. Fixed-price quotation.
- 2. Proposed test window.
- 3. Engagement-team profile (anonymised CVs acceptable).
- 4. Sample executive summary from a prior comparable engagement (anonymised).
- 5. Confirmation of insurance and certifications.

Quotations to: [founder contact].

11. Selection criteria

Criterion	Weight
Quality of sample executive summary	30%
Channel Islands / UK FS pen-test track record	25%
Fixed-price competitiveness	20%
Engagement-team certifications	15%
Proposed test window fit	10%

12. After award

- Pen-test executive summary becomes a canonical deliverable referenced by `06_DPIA_Template`, `07_BCP_Outline`, every pilot agreement, and every customer security questionnaire response.

- Logged in `/docs/canonical/security-artefacts/` with annual refresh diary.
- Findings categorised into `07-known-gaps.md` triage: "must fix pre-pilot", "must fix pre-Bespoke", "tolerable forever".
