RegAlign®

Chain Verifier — Auditor Runbook

Audience: External auditor, internal audit, audit-committee chair, or supervisory authority running an independent integrity check of a RegAlign® tenant's hash-chained audit trail.

Time required: 10 minutes for a first check; 2 minutes for a repeat.

Access required: A modern browser. No RegAlign login. No credentials. No NDA.

What you are verifying

Every audited event in a RegAlign tenant is hash-linked to its predecessor. Tampering with any historical entry breaks the chain at that point. The public verifier walks the entire chain server-side and returns one of two outcomes:

- **Chain intact** — every entry hashes to the value stored in its successor. The full audited history is byte-identical to what was sealed at the time of writing.
- **Chain broken** — the verifier identifies the entry ID at which the break occurs. The tenant's audited history cannot be trusted from that point forward.

The verifier returns only the pass/fail result and the entry ID of any break. It does not return event payloads, actors, or content — your independence is preserved without your having to read the underlying records.

Step-by-step

1. Obtain the tenant ID

Ask the firm for its **RegAlign tenant ID** — a UUID in the form `00000000-0000-0000-0000-000000000000`. It is not a secret.

2. Open the public verifier

Navigate to `https://regalign.app/verify`. There is no sign-in screen.

3. Paste the tenant ID and click Verify chain

The server-side check typically completes in under a second. Rate-limited to 10 checks per tenant per minute.

4. Read the result

Chain intact shows entries checked, first hash, and last hash (the chain root at the moment of your check). Record all three.

Chain broken shows entries checked before the break and the entry ID at which the break was detected. This is a finding — record and report.

5. Cross-check against a sealed export

Sealed exports (board packs, period evidence packs, regulator responses) carry a chain root in their footer. Confirm it matches *Last hash* from the verifier at the time of export. A match proves the export is byte-identical to the audited reality at that moment.

Working-papers template

Item	Value
Date / time of check (UTC)	
Auditor name	
Tenant ID	
Verifier URL	https://regalign.app/verify
Result	Chain intact / Chain broken
Entries checked	
First hash	
Last hash (chain root at check)	
Sealed-export root cross-checked?	Yes / No / N/A
Match?	Yes / No / N/A
Findings	

What this does NOT test

The verifier proves **integrity** — that the audited history has not been tampered with after the fact. It does not test whether the firm captured the right events in the first place, whether the firm's controls are designed effectively, whether the firm's evidence is complete, or who authored the original events. Use other audit procedures for those.

A clean chain means the firm cannot have quietly edited the past. It does not mean everything in the past was done correctly.

What to do if the chain is broken

A broken chain indicates one of: tampering, storage corruption, or a deployment defect in the hashing or write path. In all three cases the firm must investigate root cause and report findings to its board and supervisor as appropriate. RegAlign provides root-cause analysis support on request and publishes a transparency report if the defect is in our code.

Frequency

- **Quarterly** as part of routine audit-committee oversight.
- **Before sealing** any board pack, period evidence pack, or regulator response.
- **On demand** whenever a stakeholder questions the integrity of the audited history.

Each check is rate-limited but otherwise free and unmetered.

Reporting issues

If the verifier itself is unavailable, returns an unexpected error, or you have any concern about the result, contact **trust@regalign.app**. Confirmed verifier-side defects are disclosed on the public Trust Centre at `regalign.app/trust`.