THINKING OS™

SEAL Diligence Brief

Straight Answers to the Trust Questions

Public • v1.0 • April 2026

Doc ID: TOS-SEAL-DB-v1.0-7p8v

Document: SEAL Diligence Brief
Version: v1.0 (Public) – April 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

Table Of Contents

Doc ID: TOS-SEAL-DB-v1.0-7p8v

Document: SEAL Diligence Brief
Version: v1.0 (Public) – April 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

SEAL is a pre-execution governance runtime for designated legal workflows. It sits in front of a governed action boundary and returns **approve, refuse, or supervised** before that action leaves the firm. It is delivered as a **vendor-hosted sealed API**, not as a drafting tool, dashboard, or general-purpose legal platform.

This brief is intended to answer the trust questions a serious buyer asks before deeper diligence.

1. Is SEAL vendor-hosted?

Yes. SEAL is delivered as a **vendor-hosted sealed API**. Your systems call it through an authenticated integration surface; SEAL returns governed outcomes and decision artifacts. The deployment model is hosted refusal infrastructure, not traditional software installed inside your environment.

2. Why are the internals sealed?

Because the assurance model is **inspectable outputs, not exposed internals**. Regulators, auditors, and buyers test SEAL by sending scenarios and reviewing sealed outputs, not by inspecting prompts, models, or rule internals. This protects both your IP and Thinking OS IP while still providing reviewable evidence at the moment of action.

3. Is there an on-prem version?

The current deployment model is a vendor-hosted sealed API. Standard access is hosted, not customer-operated. No right to host SEAL internals in your environment is granted unless separately agreed in writing.

4. What data does SEAL actually see?

SEAL works at the edge. It sees the **minimum structured inputs required to govern the action**: who is acting, what action is being attempted, in what legal context, under what authority or consent posture, and any configured evidence or authority metadata. SEAL does **not** require database or DMS access, does **not** ask for prompt access or model tuning, and does **not** become the system of record. Raw identity and authority tokens are not stored in the artifact itself; the artifact preserves the stable identifiers and summaries needed for audit and later review.

Doc ID: TOS-SEAL-DB-v1.0-7p8v

Document: SEAL Diligence Brief
Version: v1.0 (Public) – April 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

5. Is our data used to train models?

No. SEAL does **not** use client artifacts or matter data to train public models or improve other clients' systems, and subprocessors are expected to operate under the same no-training posture where used.

6. Who owns policy?

You do. The firm remains responsible for:

- policies and authority rules
- identity and role sources
- matter and workflow selection
- legal judgment and professional supervision

SEAL **does not invent roles or policy** and does not determine which filings are lawful, advisable, or ethically required. It enforces the firm's written rules under the firm's supervision.

7. Who owns artifacts?

SEAL decision artifacts are produced for the client's matters and workflows and are designed for client-controlled, append-only retention with integrity controls. Firms may direct artifacts into their own storage perimeter and set retention policies.

Thinking OS owns the runtime internals; the client retains control of its policies, workflows, and underlying legal work.

Client artifacts are encrypted in transit and at rest, and Thinking OS personnel access is restricted to audited support and incident-response functions under role-based controls.

8. What is actually in scope?

Only the workflows you choose to wire through SEAL are in scope. The list of workflows routed through the gate is the **Coverage Map**. If a workflow is not wired through the gate, it is not governed by SEAL. This is why pilots start narrow:

- one named workflow
- one named owner
- one agreed posture
- one review cadence

9. What happens if SEAL is wrong?

SEAL does not replace legal judgment. It enforces the configuration and policy posture supplied for the workflow in scope. If an outcome looks wrong, the artifact shows which anchors, roles, scopes, and authorizations were in force so the firm can correct its own configuration, routing, or policy posture. If Thinking OS becomes aware of a defect that could materially affect approvals or refusals, affected clients are notified and remediation is coordinated.

Firms are still expected to maintain human checks for critical deadlines and filings. SEAL is one control among many, not a claim that “the system is always right.”

10. What happens if the gate is down?

The design philosophy is **no silent degradation**. If SEAL cannot safely evaluate a request, it returns a sealed refusal or error family rather than silently allowing ungoverned action to continue unseen. Malformed payloads, missing consent, ambiguous identity, unknown roles, unreachable providers, and similar unsafe states fail closed rather than pass through quietly.

Operational SLAs and business-continuity fallbacks belong in the commercial agreement and your own continuity planning, but the runtime stance is clear: **unsafe evaluation does not become silent approval**.

11. How do we start without blocking everything?

Through staged access. Three access paths:

- **Confidential Evaluation**: bounded, vendor-hosted, no client integration required
- **Wired Pilot**: one named workflow, observe-only or active enforcement
- **Licensed Enforcement**: production use for agreed in-scope workflows

That means you can start with:

- no production workflow change
- one named workflow
- observe-only / shadow mode first
- pause or rollback under the pilot charter

12. Can we defend this to insurers, courts, or a risk committee?

Yes — that is one of the main reasons the runtime exists. Every governed decision produces a sealed artifact with:

- decision / trace reference
- integrity-verifiable artifact reference
- governance anchors in force
- governing policy or rule-basis reference
- code family and human-readable rationale

Artifacts are designed to support:

- malpractice defense
- bar or regulator packets
- internal investigations
- audit and compliance review

The defensible narrative is straightforward:
"We had a governed, pre-execution control enforcing our policies at the moment of action."

13. Does SEAL replace our GRC, IdM, or matter systems?

No. You retain and continue to improve your own:

- policies
- role definitions
- identity and matter systems

SEAL's job is to enforce what those systems assert at runtime and prove that it did so, without becoming your system of record.

14. Does SEAL draft, file, or provide legal advice?

- SEAL never drafts or files
- SEAL does not provide legal advice
- approvals are governance pre-conditions, not certifications of legal merit,

strategy, or ethical sufficiency
- attorneys remain fully responsible for decisions and filings

15. What are Thinking OS's responsibilities?

Thinking OS is responsible for:

- correct operation of the runtime within agreed scope
- faithful enforcement of the configuration in place
- production of integrity-verifiable decision artifacts
- runtime security, availability, and isolation

16. What are the client's responsibilities?

The client remains responsible for:

- who is allowed to act
- which motions or actions are permitted, advisory-only, or blocked
- maintaining those rules as law and policy evolve
- choosing which workflows route through SEAL
- monitoring queues and treating unusual patterns as incident signals
- maintaining human supervision and deadline controls

Bottom line

SEAL is not asking you to believe in a vague category. It is offering a bounded governance control with a specific operating model:

- **vendor-hosted**
- **sealed internals**
- **client-owned policy and identity**
- **tenant-owned reviewable artifacts**
- **fail-closed behavior**
- **observe-first pilot path**
- **clear pause / rollback path**
- **defensible evidence for risk, insurers, courts, and regulators**

Public evaluation reference. Redacted.

Describes evaluator-visible behavior and evidence surfaces only; no non-public runtime details are included.

For information only. Not legal advice.