THINKING OS™

SEAL Diligence Brief

Straight Answers to the Trust Questions

Public • v1.1 • May 2026

Doc ID: TOS-SEAL-DB-v1.1-7p8v

Document: SEAL Diligence Brief
Version: v1.1 (Public) – May 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

Table Of Contents

SEAL Legal Runtime is a pre-execution authority gate for designated high-risk legal workflows. It sits at the Commit Layer: the moment before a governed filing, submission, approval, or other high-risk legal action leaves the firm or binds the institution. It returns approve, refuse, or supervised override before the governed action proceeds.

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.

Doc ID: TOS-SEAL-DB-v1.1-7p8v

Document: SEAL Diligence Brief
Version: v1.1 (Public) – May 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

4. What data does SEAL actually see?

SEAL works at the edge. It sees the **minimum structured governance signals** required to evaluate the governed action: who is acting, what action is being attempted, what workflow or legal environment is involved, under what authority or consent posture, and any configured evidence, deadline, or rule-basis reference.

SEAL does not require full matter text, database access, DMS access, model prompts, model traces, privileged strategy, or legal advice content.

SEAL does not become the system of record. The artifact preserves the stable identifiers, outcome, reason category, and review references needed for audit and later review.

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.

The firm's retention, export, post-termination access, verification support, and artifact review rights should be defined in the written agreement. Thinking OS™ does not claim ownership of the firm's identity data, matter context, or decision artifacts. Any post-termination verification support, export process, or vendor-operated review support should be expressly defined in the written agreement.

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

Coverage is explicit, not implied. SEAL does not claim universal control across the firm.

If an action can still execute outside SEAL, that path is out of scope until the firm brings it under workflow control.

Doc ID: TOS-SEAL-DB-v1.1-7p8v

Document: SEAL Diligence Brief
Version: v1.1 (Public) – May 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

9. What if our authority, role, or matter data is incomplete?

SEAL depends on the structured signals the firm provides for the governed workflow.

It does not make inaccurate source data accurate.

In observe-only mode, stale roles, missing authority, inconsistent matter context, unclear consent, or incomplete supervision signals become review findings, not production blockers.

That is one reason the first pilot starts observe-only. The firm can see whether its authority signals are ready before any refusal category moves into controlled enforcement.

The firm decides whether signal quality is ready for enforcement.

10. 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 governance signals, roles, scope, authority posture, and policy or rule-basis references 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.”

In observe-only mode, questionable outcomes become review findings, not production blockers.

Doc ID: TOS-SEAL-DB-v1.1-7p8v

Document: SEAL Diligence Brief
Version: v1.1 (Public) – May 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

11. What happens if the gate is down?

In observe-only mode, SEAL does not block production users. It records what it would have approved, refused, or routed for supervision.

In controlled enforcement, the design posture is no silent degradation. If SEAL cannot safely evaluate a governed request, the runtime should refuse or route for supervision instead of silently allowing an unevaluated action to proceed.

Operational SLAs, continuity procedures, fallback paths, and escalation rules belong in the written agreement and the firm's business-continuity planning.

Unsafe uncertainty should not become invisible approval.

12. How do we start without blocking everything?

The first design-partner motion starts observe-only.

The initial evaluation is intentionally narrow:

- one law firm
- one workflow
- one final-submit checkpoint
- observe-only first
- no production blocking in Phase 1
- no rip-and-replace

SEAL records what it would have **approved, refused, or routed for supervision** before the firm decides whether any refusal category should move into controlled enforcement.

Controlled enforcement is a separate decision and requires scoped review, authority mapping, integration review, security review, and written agreement.

13. Does SEAL need to integrate directly with ECF or the court portal?

No — not for the first observe-only evaluation.

The first pilot evaluates the firm-controlled workflow boundary before external submission. SEAL receives a structured intent to act and records what it would have approved, refused, or routed for supervision.

Production enforcement is a separate decision. If the firm later wants enforcement, the exact wiring point is scoped with the firm or workflow vendor so the governed path requires a SEAL outcome before the filing proceeds.

SEAL does not replace the filing system, court portal, matter system, DMS, GRC platform, or routing engine.

14. Can this support insurer, court-facing, regulator, or risk committee review?

Yes. One purpose of the runtime is to preserve reviewable evidence of what the control did at the moment of action.

Every governed decision produces a sealed artifact with:	**Artifacts are designed to support:**
• decision / trace reference • integrity-verifiable artifact reference • governance signals in force • governing policy or rule-basis reference • reason category and human-readable rationale	• internal risk review • insurer review • audit and compliance review • bar, regulator, or malpractice-related scrutiny where appropriate • matter-level governance review

The defensible narrative is straightforward:

"We had a governed, pre-execution control applying our configured authority posture at the moment of action, and we retained a reviewable decision artifact showing what the control did."

15. Does SEAL replace our GRC, IAM, or matter systems?

No. You retain and continue to improve your own:

- policies
- role definitions
- identity and matter systems

SEAL's job is to apply the configured authority posture at runtime and preserve reviewable evidence of the governed outcome, without becoming your system of record.

16. 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

17. What are Thinking OS's responsibilities?

Thinking OS is responsible for:

- correct operation of the runtime within agreed scope
- applying the configured authority posture for scoped governed workflows
- production of integrity-verifiable decision artifacts
- maintaining the runtime's security, integrity, availability, and isolation posture within the agreed scope and written agreement

18. 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

19. What happens near a deadline?

Deadline pressure should not become permission to bypass governance.

If a governed request is refused near a deadline, SEAL is designed to preserve the refusal, surface the deadline context, and support a firm-owned escalation path.

The firm owns the supervisor path, after-hours review posture, fallback procedure, and routing destination.

Deadline-sensitive refusal categories should not move into controlled enforcement until the firm has defined who reviews them, how quickly they must be reviewed, and what fallback procedure applies.

Bottom line

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

- vendor-hosted sealed runtime
- sealed internals
- client-owned policy and identity sources
- client-controlled reviewable artifacts
- scope-bounded coverage
- observe-only first
- no production blocking in Phase 1
- controlled enforcement only by written scope
- defensible evidence for risk, insurer, audit, and regulatory review where appropriate

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.