THINKING OS™

SEAL Diligence Brief

Straight Answers to the Trust Questions

Public • v1.2 • August 2026

Doc ID: TOS-SEAL-DB-v1.2-7p8v

Document: SEAL Diligence Brief
Version: v1.2 (Public) – August 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 runtime for scoped legal actions. For the 30-day Observe-Only Final-Submit Review, SEAL evaluates one designated final-submit boundary using the firm's configured authority posture and records what would have been approved, would have been refused, or routed for supervision.

During the review, no production filing is blocked, delayed, or altered. Any later controlled enforcement is separately scoped and separately approved.

Existing firm systems remain the sources of truth for identity, matter context, policy, authority, consent, supervision, and related governance facts.

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.

Doc ID: TOS-SEAL-DB-v1.2-7p8v

Document: SEAL Diligence Brief
Version: v1.2 (Public) – August 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

1. Where exactly does SEAL sit, and what invokes it?

SEAL sits at the final-submit boundary for one designated workflow: the point immediately before the filing or submission is released externally.

The invoking system is firm-specific. It may be a filing workflow, docketing workflow, matter workflow, or another firm-controlled system that owns the final-submit event.

That workflow supplies a structured intent to act containing the minimum agreed governance signals. SEAL evaluates the request and records the governed finding and decision artifact.

During the 30-day review, the SEAL finding is observe-only and non-enforcing.

2. 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 current deployment model is vendor-hosted SEAL Legal Runtime, not traditional customer-operated software installed inside the firm's environment.

3. Why are the internals sealed?

Because the evaluation model is evaluator-visible behavior and evidence, not exposed implementation internals.“Sealed” does not mean unverifiable. It means the governed behavior and evidence surface can be evaluated without exposing proprietary runtime internals.

A qualified evaluator can review the governed scenario, returned finding, decision identity, context anchors, policy or rule-basis linkage, trace reference, and integrity indicators.

The evaluator does not need access to proprietary implementation logic, internal policy mechanisms, credentials, raw tokens, or code-level architecture to determine what the control recorded. **Sealed behavior is evaluator-visible behavior, not hidden behavior.**

4. 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.

5. What data does SEAL actually see?

SEAL evaluates only the minimum structured governance signals required for the scoped review. Those may include:

- actor identity;
- trusted role or group;
- workflow and attempted action;
- client, matter, and docket identifiers where required;
- authority / consent / evidence posture;
- deadline or urgency where material.

SEAL does **not** require full matter text, full DMS or database access, model prompts, model traces, privileged strategy, passwords, raw credentials, private signing keys, or unrelated legal-advice content merely to conduct the review.

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.

6 Is our data used to train models?

No. Thinking OS does not use client artifacts, matter data, or decision records to train public models or improve other clients' systems.

Where subprocessors are used, their applicable data handling, confidentiality, retention, and no-training obligations are addressed through the relevant contractual and diligence terms.

7. Who owns policy?

The firm does.

The firm defines and approves its policy posture, authority rules, identity and role sources, matter context, supervision model, and legal judgment.

SEAL does not decide who should be authorized as a matter of law or firm policy.

During the observe-only review, SEAL evaluates the supplied governance request against the firm's configured authority posture and records the finding.

Only under separately approved controlled enforcement can the governed outcome become authoritative for an agreed wired path.

8. Who owns artifacts?

The firm owns its decision artifacts as firm business records and controls their retention, review, privilege, confidentiality, use, and disclosure posture.

Thinking OS retains ownership of SEAL Legal Runtime, its proprietary internals, and implementation IP.

Artifact storage and custody are deployment-specific. The applicable agreement should define storage location, export, deletion, post-termination access, verification support, and any client-controlled retention requirements.

Decision artifacts are designed with integrity controls and evaluator-visible evidence references. Thinking OS does not claim ownership of the firm's policies, legal work, matter data, authority model, or decision records.

9. How can an evaluator review artifact integrity?

A decision artifact is designed to expose a stable decision identity, timestamp, governed finding, relevant context anchors, policy or rule-basis references, trace or correlation references, and integrity-verifiable evidence references.

A qualified evaluator should be able to sample governed findings and confirm that each artifact corresponds to a specific decision, specific context, and specific policy posture.

The artifact does not prove that the firm's policy was legally correct, that upstream data was accurate, that every firm workflow was governed, or that the filing itself was legally sufficient.

Deployment-specific verification mechanics, retention, export, and post-termination verification support belong in written diligence or the applicable agreement.

10. What is actually in scope?

The 30-day review covers one designated workflow and one designated final-submit boundary.

The agreed written scope identifies the workflow, actors / roles, authority conditions, signal sources, review cadence, and explicit exclusions.

SEAL does not claim universal control across the firm.

During the observe-only review, findings are non-enforcing.

If controlled enforcement is later separately approved, SEAL can be non-bypassable only within the **agreed workflow path wired to require a SEAL outcome**. Any alternate route outside that path remains outside SEAL's claimed control surface.

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

SEAL does not turn missing or contradictory required governance facts into silent approval.

If required identity, role, matter, docket, action, authority, consent, evidence, or deadline context is missing, stale, mismatched, contradictory, or cannot be safely evaluated, SEAL records the applicable would-have-refused or supervised-review finding under the configured review posture.

During the 30-day review, that finding does not block, delay, or alter the production filing."

The purpose is to let the firm determine whether its governance signals are sufficiently reliable before any controlled enforcement is considered.

12. Does a SEAL approval mean the filing is legally correct?

No.

During the observe-only review, a Would Have Approved finding means the request satisfied the firm's configured authority conditions under the governance facts supplied for the scoped action.

It does **not** mean that the filing is legally correct, strategically wise, ethically sufficient, jurisdictionally proper, or professionally advisable.

Lawyers and supervisors remain responsible for legal judgment and professional obligations.

Approval means "authorized under configured conditions," not "legally correct."

13. What happens if SEAL is wrong?

During the 30-day review, a questionable SEAL finding is a review issue, not a production blocker.

The decision artifact is designed to show the relevant governance facts, authority posture, reason category, and policy or rule-basis surface so the firm can determine whether the issue came from source data, configuration, policy ambiguity, or the runtime.

The firm remains responsible for correcting its own policy, identity, authority, or source-system facts.

If Thinking OS identifies a runtime defect that could materially affect governed findings, Thinking OS is responsible for coordinating the appropriate remediation within the agreed scope.

SEAL is a control. It is not a claim that the system is always right.

14. What happens if the gate is down?

During the 30-day observe-only review, SEAL is not a production filing dependency.

If SEAL is temporarily unavailable, the firm's existing production filing process remains in control. An affected event may not receive a SEAL finding or artifact. Any known observation gap should be treated as part of the review record and examined during the agreed review cadence.

If the firm later considers controlled enforcement, the posture changes. A governed request should not silently proceed merely because the authority control is unavailable.

Availability commitments, fallback procedures, continuity rules, escalation paths, and any fail-closed behavior for production enforcement must be separately defined in writing before enforcement is activated.

15. How do we start without enforcing everything?

Start with one 30-day Observe-Only Final-Submit Review.

The initial review is deliberately bounded:

- one firm;
- one named workflow;
- one final-submit boundary;
- one workflow owner;
- one weekly review cadence;
- the minimum agreed governance signals;
- Observe-Only / Non-Enforcement posture.

No production filing is blocked, delayed, or altered during the review.

At the end, leadership receives the decision artifacts, final risk ledger, and recommendation and chooses whether to stop, continue observing for a defined reason, improve signals, or consider one narrow controlled-enforcement path under separate written scope.

The review ends with a decision, not an automatic deployment.

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

No—not for the 30-day observe-only review.

The review focuses on the firm-controlled workflow boundary immediately before external submission. The firm-controlled workflow that owns that event supplies SEAL with the agreed structured governance request.

SEAL does not replace ECF, the court portal, filing software, DMS, matter systems, IAM, GRC, or routing systems.

If controlled enforcement is later considered, the exact production wiring point must be separately identified so the agreed governed path can require a SEAL outcome before the action proceeds.

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

The decision artifacts are designed to support later review by the firm and, where the firm chooses, by risk, insurers, auditors, outside counsel, regulators, or other oversight functions.

The firm controls privilege, confidentiality, retention, disclosure, and external use.

A SEAL artifact is evidence of what the control recorded or decided under the supplied governance facts and configured posture.

It is not legal advice, does not prove the firm's policy was legally correct, and is not a claim of automatic court admissibility or evidentiary sufficiency.

Any court-facing or regulator-facing use remains subject to matter-specific legal judgment.

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

No.

Your existing systems remain sources of truth for identity, roles, policy, matter context, authority, consent, supervision, and related governance facts.

During the 30-day review, SEAL evaluates those structured facts at the final-submit boundary and records the governed finding.

SEAL does not become your DMS, IAM, GRC, matter system, filing system, docketing platform, workflow engine, or system of record.

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

- **SEAL does not draft, sign, send, submit, or file legal work on its own.**
- SEAL does not provide legal advice or legal judgment.
- During the observe-only review, a **Would Have Approved** finding means only that the configured authority conditions were satisfied under the supplied governance facts.
- It is not a certification of legal merit, strategy, ethical sufficiency, or jurisdictional correctness.
- Lawyers and supervisors remain responsible for decisions and filings.

20. What are Thinking OS's responsibilities?

Thinking OS — Thinking OS is responsible for:

- operating SEAL Legal Runtime within agreed review scope;
- faithfully returning governed findings for the scoped review;
- producing reviewable decision artifacts;
- maintaining the runtime's security, integrity, and availability posture within agreed scope;
- supporting the agreed bounded integration and evaluation path;
- supporting the agreed evidence package and review cadence.

21. What are the firm's responsibilities?

Firm — The firm remains responsible for:

- policies and authority rules;
- identity and role sources;
- matter and workflow context;
- authority / consent sources;
- deadline and urgency sources;
- supervision;
- workflow routing and escalation;
- legal judgment;
- professional responsibility;
- decision-record retention and disclosure decisions;
- whether anything beyond observe-only review is considered.

22. What happens near a deadline?

Deadline pressure does not become permission.

During the observe-only review, deadline and urgency facts supplied by firm-controlled systems may be preserved in the finding and artifact, but SEAL does not disrupt the production filing.

The firm owns deadline calculation, calendaring, supervisor selection, review timing, after-hours procedures, and fallback.

No deadline-sensitive refusal condition should move into controlled enforcement until those responsibilities are explicitly defined.

23. What does the $40,000 fixed-fee review include?

The $40,000 fixed fee covers one 30-day Observe-Only Final-Submit Review of one designated workflow and one final-submit boundary.

It includes:

- review scoping and charter;
- minimum signal mapping;
- bounded workflow and signal review;
- weekly review sessions;
- decision artifacts for governed attempts;
- final risk ledger;
- leadership recommendation.

It does **not** include production enforcement, firmwide rollout, multi-workflow coverage, replacement of existing systems, legal advice, or access to SEAL runtime internals.

The fee buys a controlled evaluation and evidence package, not a software trial.

24. What proof do we receive after 30 days?

The 30-day review is intended to produce:

- Review Scope Memo / Charter;
- Minimum Signal Map;
- weekly review sessions;
- reviewable decision artifacts;
- final risk ledger;
- leadership recommendation.

The fee buys a controlled evaluation and evidence package, not a software trial.

25. What assurance exists today?

SEAL has controlled evaluator evidence, founder-led hostile review, and pre-diligence testing of the scoped final-submit control.

Thinking OS does not represent that work as a third-party security audit, penetration test, SOC 2 report, certification, or customer production deployment.

Any required independent security assessment, assurance roadmap, DPA, security schedule, subprocessor review, insurance evidence, or production-specific continuity commitment belongs in deeper diligence before controlled enforcement.

26. Has a law firm deployed this yet?

Thinking OS is not claiming a customer production deployment.

Current evidence comes from **controlled evaluator testing and the External Proof Packet.**

The purpose of the 30-day observe-only review is to evaluate the control against one real firm workflow before any production enforcement is considered.

27. What moves into deeper diligence?

This public brief is intended to provide a clear understanding of the product boundary, review posture, evidence model, and current assurance claims.

Deeper written diligence may include, as applicable:

- exact contracting entity and corporate information;
- insurance certificates and current coverage;
- security controls schedule;
- DPA and subprocessor schedule;
- deployment-specific data handling and retention;
- independent security assessment status;
- availability and business-continuity commitments;
- confidential artifact-verification procedures;
- production support and escalation responsibilities;
- corporate IP ownership confirmation.

Thinking OS does not improvise those facts from memory or substitute public positioning language for formal diligence documentation.

Bottom line

SEAL Legal Runtime is being offered first as a **30-day Observe-Only Final-Submit Review** of one designated filing workflow.

The posture is deliberately bounded:

- vendor-hosted sealed runtime;
- one final-submit boundary;
- firm-owned policy and authority posture;
- existing systems remain sources of truth;
- minimum structured governance signals;
- reviewable decision artifacts;
- observe-only / non-enforcement review;
- no production filing blocked, delayed, or altered;
- no claim of universal control across the firm;
- no claim that approval means legal correctness;
- no automatic path to enforcement;
- controlled enforcement only under separate written scope and firm approval.

The purpose of the public diligence brief is not to eliminate deeper diligence. It is to give a serious buyer an accurate mental model of what SEAL is, what it is not, what can be evaluated now, and what requires further written review.

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.