THINKING OS™

SEAL Final-Submit Review Charter

Wrong-Authority Filing Risk at the Final-Submit Boundary

Public Template · v1.2 · August 2026

Document: SEAL Final-Submit Review Charter
Version: Public Template · v1.2 · August 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

THINKING OS™

Review Information

Document Version: v1.2 **Date:** ________________________ **Participant / Firm:** _____________ **Review Name:** ________________	**Workflow Owner:** ___________________ **Legal / Risk Owner:** ________________ **Technical Contact:** __________________ **Security / IAM Contact:** _____________ **Thinking OS Review Lead:** ___________ **Review Type:** 30-Day Observe-Only **Enforcement During Review:** No

1. Purpose of This Review

This review is designed to evaluate **one narrow governance control in one designated legal filing workflow**.

SEAL Legal Runtime evaluates one final file / submit workflow for one buyer-selected motion or submission type and records what **would have been approved, would have been refused, or routed for supervision** under the firm's configured authority posture before the filing leaves the firm.

The review is not intended to:

- replace the firm's filing system, DMS, matter system, IAM, GRC, docketing system, or workflow tools;
- evaluate all legal work;
- change legal practice across the firm;
- provide legal advice or legal judgment;
- or activate production enforcement.

The review is intended to answer one operational question:

> **Can the firm obtain a useful, reviewable authority decision at one final-submit boundary before a filing leaves the firm—without blocking, delaying, or altering production filings during the 30-day review?**

The review is deliberately narrow, bounded, and reversible.

2. Governed Workflow in Scope

Motion or submission type:
[Buyer-selected motion or submission]

Governed workflow:
[Named filing / docketing / matter / submission workflow]

Final-submit boundary:
[The exact step immediately before the filing or submission is released externally]

Source workflow or system:
[Workflow tool / filing tool / docketing system / matter system / other]

Environment used for observation:
[Agreed evaluator / test / production-adjacent / limited live observation posture]

Named workflow owner:
[Name / Title]

The review covers **one designated workflow and one designated final-submit boundary only**.

No other workflow, practice group, motion family, action class, or execution path is included unless added by written amendment or separate written scope.

3. Primary Control in Scope

The primary control evaluated at the start of the review is:

Wrong Authority / Role Not Authorized

The core question is:

> **If the wrong actor appears at the designated final-submit boundary under the wrong authority, does SEAL identify and record that condition before the filing leaves the firm?**

The review does not begin with a broad governance taxonomy.

It begins with the minimum control condition necessary to evaluate whether the authority boundary is useful.

4. Would-Have-Refused Conditions in Scope

Primary condition at review start

- wrong authority / role not authorized

Additional conditions that may be included only by agreement

- role disallowed or structurally barred actor;
- required authority condition missing, invalid, stale, mismatched, or otherwise not satisfied;
- required consent or evidence condition missing or invalid;
- supervised-review condition required.

Additional conditions do not automatically become part of the review merely because SEAL is technically capable of evaluating them.

Any added condition must be deliberately agreed within the scoped review.

5. Actors and Roles in Scope

The review may include human or machine actors that genuinely appear in the designated workflow.

Initiating actors or roles may include

- [Partner]
- [Attorney]
- [Paralegal]
- [Docketing / Litigation Support]
- [Legal Ops / Innovation]
- [Service Account]
- [Filing Automation]
- [AI / Workflow Agent]
- [Other: ________________________________]

Supervisory roles may include

- [Partner]
- [General Counsel]
- [Practice Lead]
- [Other: ________________________________]

Explicitly out of scope

- actors and roles not included in the agreed review configuration;
- unrelated workflows;
- unrelated motion or submission types;
- alternate filing paths not part of the designated observed workflow.

SEAL applies the authority question to the actor presented by the firm's trusted governance signals. It does not treat a self-declared workflow role as authoritative merely because it appears in the request.

6. Firm-Owned Sources of Truth

The firm remains the source of truth for:

- policies and authority rules;
- identity and trusted role / group sources;
- matter and docket context;
- workflow context;
- consent and authority records;
- supervision posture;
- deadline and urgency information;
- legal judgment and professional responsibility;
- artifact retention, review, use, privilege, confidentiality, and disclosure decisions.

SEAL does not replace those systems or invent institutional facts merely to complete a decision.

SEAL evaluates the structured governance signals supplied for the designated workflow against the firm's configured authority posture.

SEAL does not make inaccurate source data accurate.

If a required source fact is stale, missing, conflicting, unclear, or otherwise not safely evaluable, that condition remains visible in the review rather than being silently converted into approval.

7. Minimum Governance Signals

The firm and Thinking OS will identify the minimum signals required for the scoped review.

Depending on the agreed workflow, those signals may include:

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

The review should use the **minimum structured governance information necessary** for the scoped authority decision.

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

A separate Technical Signal Map may be used to identify the source system, owner, field, and readiness posture for each required signal.

8. Review Posture

The 30-day review operates in:

Observe-Only / Non-Enforcement Mode

During the review:

- the designated workflow is evaluated by SEAL;
- SEAL records what would have been approved, refused, or routed for supervision;
- reviewable decision artifacts are produced for governed attempts as configured;
- the firm reviews outcomes against its own intended authority posture;
- the review remains non-disruptive.

During the 30-day observation period:

> **SEAL does not block, delay, or alter production filings.**

A governance finding of **Would Have Refused** is therefore a real review finding.

It is **not** a claim that SEAL production-disrupted the filing.

The purpose of observe-only review is to let the firm examine:

- signal quality;
- authority mapping;
- refusal patterns;
- supervised-review findings;
- artifact usefulness;
- and workflow fit

before deciding whether anything further is justified.

Nothing moves into controlled enforcement automatically.

9. Governed Review Outcomes

During the observe-only review, SEAL may record:

Would Have Approved

The governed request appears to satisfy the configured authority conditions for the scoped action.

Would Have Refused

The governed request does not satisfy one or more required authority conditions.

Routed for Supervision

The governed request presents a condition that the firm has configured for supervised review rather than ordinary would-have-approval.

These are governance findings for the scoped review.

They do not represent legal advice or legal correctness.

A Would Have Approved finding means only that the configured authority conditions for the scoped action were satisfied under the supplied governance facts.

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

Lawyers and supervisors remain responsible for those judgments.

10. Supervised Review

The firm owns its supervision process.

During the 30-day observe-only review, SEAL may record that an action **would have required supervision**.

SEAL does not:

- select the supervisor;
- create a ticket or queue;
- assign work;
- operate the firm's review workflow;
- or approve an exception on behalf of the firm.

If controlled enforcement is later separately approved, any formal supervised exception path must be separately defined and authorized.

Where such a path is used, the design objective is to preserve the original refusal and separately record the later authorized supervisory decision.

> **Supervision is not a silent bypass.**

11. Deadline-Sensitive Findings

Deadline pressure does not become permission.

Where deadline or urgency context is relevant and supplied by firm-controlled systems, SEAL may preserve that context in the governed finding and decision artifact.

During the observe-only review:

- deadline-sensitive findings remain non-enforcing;
- the firm owns deadline calculation and calendaring;
- the firm owns escalation timing and review ownership;
- the firm owns any after-hours or fallback procedure.

A deadline-sensitive refusal category should not move into controlled enforcement unless the firm has separately defined:

- who reviews it;
- the applicable review window;
- fallback if that reviewer is unavailable;
- what happens if the issue remains unresolved;
- and whether any authorized supervised path is permitted.

12. What the Review Does Not Do

This review does not:

- provide legal advice;
- decide legal strategy;
- determine whether a filing is legally correct;
- determine whether a filing is ethically required or professionally advisable;
- replace lawyers or professional supervision;
- replace the filing system;
- replace the court or regulator portal;
- replace the DMS;
- replace the matter system;
- replace IAM or identity systems;
- replace GRC or policy systems;
- replace docketing or deadline systems;
- become the system of record for the matter;
- create firm policy or authority rules;
- create tickets, queues, or supervision workflows;
- activate firmwide governance;
- or authorize SEAL to draft, sign, send, submit, or file anything on its own.

SEAL can evaluate the action boundary. It does not practice law.

13. Systems and Integration Scope

In scope

- one designated workflow or integration path;
- one final-submit boundary;
- one motion or submission type;
- agreed structured governance signals;
- agreed review-output routing;
- bounded technical support necessary to conduct the review.

Out of scope

- broad production rollout;
- replacement of existing filing infrastructure;
- unrelated practice groups;
- unrelated motion families;
- multiple workflow coverage unless separately added;
- production enforcement;
- blanket firmwide control.

The observe-only review does not require the firm to replace or redesign its entire filing stack.

The review is intended to observe the firm-controlled workflow boundary before external submission.

14. Decision Artifacts and Review Evidence

For governed attempts within scope, SEAL is designed to produce reviewable decision artifacts showing, where applicable:

- the governed action;
- who or what attempted it;
- the governed outcome;
- the relevant role or authority posture;
- the applicable matter / workflow context;
- policy or rule-basis references;
- reason category;
- runtime posture;
- binding effect where supplied;
- stable decision or trace references;
- integrity-verifiable evidence references.

Artifacts support review.

They do not by themselves prove:

- that the firm's policy was legally correct;
- that upstream identity or matter data was accurate;
- that every filing path in the firm was governed;
- that a future production deployment would be non-bypassable;
- that a refusal prevented malpractice or financial loss;
- or that a filing was legally sufficient.

The firm controls its artifact retention, review, privilege, confidentiality, use, and disclosure posture.

Deployment-specific storage, export, deletion, post-termination access, and verification support are defined in the applicable written agreement.

15. 30-Day Review Deliverables

The 30-day observe-only review is intended to produce a defined evaluation and evidence package.

The review includes:

1. **Review Scope Memo / Charter**
   One workflow, one final-submit boundary, named owners, in-scope conditions, and explicit exclusions.
2. **Minimum Signal Map**
   Identification of the governance signals, source systems, and owners required for the scoped review.
3. **Weekly Review Sessions**
   Review of governed findings, artifacts, signal issues, and emerging patterns.
4. **Reviewable Decision Artifacts**
   Evidence for governed attempts within the agreed review scope.
5. **Final Risk Ledger**
   Summary of would-have-approved, would-have-refused, and supervised-review findings, including reason patterns and material signal issues.
6. **Leadership Recommendation**
   A final recommendation to stop, keep observing for a defined reason, improve signal quality, or consider one narrow controlled-enforcement path under separate written scope.

The purpose of the review is not to prove that SEAL must be deployed.

The purpose is to produce enough evidence for the firm to make an informed decision.

16. Evaluation Criteria

The review should be evaluated against a small, disciplined set of criteria.

The firm should be able to determine:

- whether the designated final-submit boundary was observed clearly;
- whether in-scope governance findings were returned consistently;
- whether wrong-authority / role-not-authorized conditions were identified as expected;
- whether findings could be distinguished from source-data or signal-quality problems;
- whether decision artifacts were understandable to workflow and risk reviewers;
- whether the artifact and observed workflow behavior told the same control story;
- whether the review remained inside agreed scope;
- whether would-have-refused findings were correct, false-positive, missing-signal, policy-unclear, or otherwise explainable;
- whether supervised-review findings were useful;
- whether leadership could understand the evidence without requiring routine engineering interpretation;
- whether existing firm controls already answered the same authority question sufficiently well;
- and whether the firm has enough information to make a clear end-of-review decision.

Optional participant-specific evaluation criteria

The purpose of these criteria is **evaluation**, not predetermined success.

A legitimate outcome of the review may be that the control should not advance.

17. Weekly Review Cadence

Recommended cadence: Weekly

Each review should examine, as applicable:

- would-have-approved findings;
- would-have-refused findings;
- supervised-review findings;
- authority or role mismatch patterns;
- missing consent / evidence / authority conditions;
- signal-quality issues;
- deadline-sensitive findings;
- any mismatch between expected and returned outcome;
- any operational issue affecting the designated workflow;
- and artifact clarity.

Primary reviewers may include

- workflow owner;
- legal / risk / GC contact;
- practice lead or designee;
- technical contact where needed;
- Thinking OS review lead.

The purpose of weekly review is not to inspect proprietary runtime internals.

The purpose is to determine whether the governed findings match the firm's intended authority posture and whether the resulting evidence is useful.

18. Pause, Narrow, and Stop Conditions

The participant may pause, narrow, or stop the review if any of the following occurs:

- the review begins affecting workflows outside agreed scope;
- the selected workflow is not ready for observation;
- required signal quality is insufficient for meaningful review;
- artifact outputs are not sufficient for evaluation;
- security or confidentiality concerns arise;
- the workflow owner becomes unavailable;
- material scope disagreement occurs;
- the participant withdraws approval for the review;
- the designated workflow is no longer available;
- or either party determines that continued review is no longer appropriate within agreed scope.

If the review is paused or stopped:

- no broader workflow change is implied;
- no firmwide dependency is created;
- no controlled enforcement is activated;
- the participant retains its prior production process.

The review is intentionally bounded and reversible.

Commercial cancellation, refund, unused-work credit, and related fee treatment are governed by the applicable SOW or commercial agreement rather than this public charter.

THINKING OS™

19. Duration and Observation Start

Readiness / Scoping Start Date: ______________________________

30-Day Observation Start Date: ______________________________

Weekly Review Dates: ______________________________

Observation End Date: ______________________________

Final Leadership Review Date: ______________________________

The **30-day observation period begins only after the designated workflow, agreed governance signals, review recipients, and required technical / security prerequisites are ready for observation.**

Pre-observation scoping, readiness, scheduling, and signal preparation do not reduce the 30-day observation period.

The review is temporary, bounded, and reversible.

Any broader or ongoing use requires separate written agreement.

20. Responsibilities and Ownership

The Firm Remains Responsible For

- policies and authority rules;
- identity and role sources;
- matter and workflow context;
- consent and authority sources;
- deadline and urgency sources;
- supervision decisions;
- workflow routing and escalation;
- legal judgment;
- professional responsibility;
- how the firm practices law;
- retention, use, privilege, confidentiality, and disclosure decisions for its decision records;
- whether anything beyond observe-only review is considered.

Thinking OS™ Remains Responsible For

- operating SEAL Legal Runtime within agreed review scope;
- faithfully returning governed outcomes 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 weekly review and agreed evidence package.

The firm owns its policies, authority model, legal work, matter/workflow context, and decision records as firm business records.

Thinking OS retains ownership of SEAL Legal Runtime, its proprietary internals, implementation logic, and related intellectual property.

This review does not transfer legal judgment or practice control to Thinking OS.

THINKING OS™

21. Optional Future Controlled Enforcement

Controlled enforcement is not included in this charter.

If the observe-only review proves useful, the firm may choose to **consider** one narrow controlled-enforcement path.

Nothing moves into enforcement automatically.

Any controlled enforcement requires separate written scope covering, at minimum:

- one agreed workflow;
- one agreed refusal category or condition;
- the authoritative policy and authority posture;
- required signal quality;
- supervision and fallback procedure;
- deadline treatment where relevant;
- security and continuity review;
- production support expectations;
- the actual governed execution path;
- and written firm approval.

Under controlled enforcement, the governed outcome may become authoritative only for the **separately agreed wired path**.

If another filing or execution route remains outside that governed path, it remains outside SEAL's claimed control surface until deliberately brought under governance.

SEAL does not claim universal non-bypassability across the firm.

> **Controlled enforcement is a separate decision, not the default destination of the review.**

22. End-of-Review Decision

At the end of the 30-day review, the firm will choose one written outcome.

1. Stop

The firm determines that the control is not useful, not ready, sufficiently addressed by existing controls, or not worth continuing.

2. Continue Observe-Only for a Defined Reason and Period

The firm identifies:

- the remaining question;
- the additional evidence needed;
- the responsible owner;
- and the next review date.

Observe-only should not continue indefinitely without a defined reason.

3. Improve Signals and Re-Review

The firm elects to improve one or more inputs such as:

- signal quality;
- authority mapping;
- workflow ownership;
- policy clarity;
- review ownership;
- or another agreed governance input

before repeating a bounded review.

4. Consider One Narrow Controlled-Enforcement Path

The firm may choose to evaluate whether one agreed refusal category in the same workflow should become authoritative under a **separate written scope and agreement**.

No automatic deployment

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

Any additional workflow, refusal condition, or broader evaluation requires written amendment or separate scope.

Participation in the review creates no obligation to expand.

---

23. Sign-Off for Review Configuration

This sign-off confirms the agreed scope and observe-only configuration for the 30-day review.

It does **not** approve production enforcement.

Participant / Firm

Authorized Signatory

Name: ________________________________

Title: ________________________________

Signature: ________________________________

Date: ________________________________

Operational Configuration Acknowledgment

Legal / Risk Owner
Name: ______________________________
Date: ______________________________

Workflow Owner
Name: ______________________________
Date: ______________________________

Technical / Security Contact
Name: ______________________________
Date: ______________________________

Thinking OS™
Name: ______________________________
Title: ______________________________
Date: ______________________________

Final Statement

SEAL Legal Runtime is being evaluated here for one narrow purpose:

> **to determine whether one final-submit workflow benefits from a reviewable authority decision before the filing leaves the firm.**

The 30-day review is observe-only and no enforcement.

The firm remains responsible for policy, supervision, legal judgment, workflow operation, and the legal action itself.

Thinking OS operates the scoped governance runtime and produces the governed findings and reviewable decision evidence.

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

Nothing moves into controlled enforcement automatically.

SEAL can evaluate and, where separately approved for controlled enforcement, refuse a governed action. SEAL does not file.