SEAL Legal Runtime External Proof Packet

Wrong-Authority Risk Before a Filing Leaves Your Firm

Controlled evaluator tests showing what SEAL approved, refused, or routed through authorized supervision before the filing path proceeded.

Public • Redacted • v4.1 • August 2026

Doc ID: TOS-SEAL-EPP-v4.1-7j5k6l

Document: SEAL External Proof Packet
Version: v4.1 (Public • Redacted) – August 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

How to Use This Packet

GC / Managing Partner — pages 4–15
The control, where it sits, what it does and does not do, and ownership.

Want to see the scenarios? — pages 16–28
Approval, wrong authority, role refusal, missing condition, and supervised recovery.

Risk / Compliance / Insurer — pages 29–50
Decision records, authority evidence, refusal behavior, and supervised-path evidence.

Technical / Security / Architecture — pages 29–59
Runtime alignment, downstream handoff, scoped-path behavior, provenance, and evaluation boundaries.

Doc ID: TOS-SEAL-EPP-v4.1-7j5k6l

Document: SEAL External Proof Packet
Version: v4.1 (Public • Redacted) – August 2026
Owner: Thinking OS™
Use: May be shared externally. For information only; not legal advice.

Table of Contents

The One Claim This Packet Tests

This packet tests one narrow question:

Can SEAL evaluate one filing action before it leaves the firm, return a governed authority decision, and leave a reviewable record of what it decided?

That is the claim.

Not whether SEAL can practice law.

Not whether the filing is legally correct.

Not whether every workflow in a law firm is governed.

Not whether this packet proves buyer-specific production readiness.

For the evaluator-controlled legal workflow shown in this packet, SEAL is tested at one final-submit boundary before the filing path proceeds.

What the tests show

Under the configured evaluator conditions:

- **Authorized filing conditions produced approval.**
- **Wrong authority produced refusal.**
- **A role that was not permitted for the action produced refusal.**
- **Missing required consent produced refusal.**
- **A refused action could change only through a separately governed supervised path with authority recorded.**
- **For the configured demo path, a direct attempt without the required governed SEAL outcome was rejected.**

Each governed outcome produced reviewable decision evidence.

What this means in plain English

The firm defines the authority rules.

SEAL does not decide legal strategy, legal merits, ethics, or whether a filing is wise.

SEAL answers a narrower question:

Is this actor authorized to take this action, in this matter, under this authority, before the filing leaves the firm?

The packet then shows the evidence behind that answer.

What this packet does not prove

This packet does **not** prove:

- that any specific law firm policy is legally correct;
- that every workflow in a buyer environment is governed;
- buyer-specific production readiness;
- production non-bypassability in a future customer environment;
- that SEAL replaces lawyer judgment, supervision, court rules, IAM, GRC, matter systems, DMS, or filing tools;
- that any buyer has deployed SEAL in production.

The exhibits are **synthetic, evaluator-controlled tests** shown with public redactions.

The proof point is narrow: SEAL can make and record an authority decision before the scoped filing path proceeds, and a qualified evaluator can inspect the resulting evidence.

Proof in Plain English — Five Things We Tested

The easiest way to read this packet is to start with the outcomes.

Thinking OS™ used **synthetic, evaluator-controlled legal filing scenarios** to test whether SEAL would make different authority decisions when the facts changed.

Here are the five core tests.

1. The filing met the required authority conditions

What happened:
The filing request had the required role, authority, consent, matter, and policy conditions.

What SEAL did:
Approved the governed action.

What the test shows:
SEAL does not refuse everything by default. When the configured authority conditions are satisfied, the governed path can proceed.

---

2. The signed authority belonged to the wrong matter

What happened:
The actor was an attorney and signed authority was present. But the authority was scoped to a different matter than the filing request.

What SEAL did:
Refused the action.

What the test shows:
Having authority is not enough. It must be authority for this matter.

SEAL evaluates whether the supplied authority matches the specific governed action and matter before the filing path proceeds.

3. The actor’s role was not permitted to take the action

What happened:
The actor was correctly identified as a paralegal, but that role was not permitted to take the governed filing action.

What SEAL did:
Refused the action.

What the test shows:
Knowing who someone is does not automatically mean they are authorized to take every action available in the workflow.

4. Required consent was missing

What happened:
The actor and filing context were otherwise in scope, but a required consent condition was not satisfied.

What SEAL did:
Refused the action.

What the test shows:
A filing can fail the authority check even when the actor and workflow otherwise appear valid.

5. A refusal could change only through an authorized supervised path

What happened:
The original governance decision was refusal. A supervising authority then used the configured supervised path with the required authority evidence.

What SEAL did:
Preserved the original refusal and recorded the authorized supervised outcome.

What the test shows:
Supervision is not a silent bypass. The original “no” remains visible, and the later authorized decision is separately recorded.

What all five tests have in common

In every scenario, the question stayed the same:

Was this actor authorized to take this action, in this matter, under this authority, before the filing path proceeded?

The facts changed.

The governed outcome changed with them.

And each outcome left reviewable decision evidence.

These are controlled evaluator tests, not customer production deployments.

The pages that follow show the underlying artifacts and technical evidence supporting these plain-English summaries.

Disclaimer: *For information only. Not legal advice. This packet is a public evaluation reference for one narrow governed workflow.*

What This Does / Does Not Prove

This packet is intentionally narrow.

It is designed to show what happened when **SEAL Legal Runtime was tested against one controlled legal filing workflow under configured evaluator conditions.**

The exhibits should be read as evidence of that scoped control behavior — **not as proof of every surrounding legal, technical, or production condition.**

What This Packet Does Prove

For the evaluator-controlled workflow shown here, the evidence demonstrates that SEAL can:

- evaluate a filing action before the configured filing path proceeds;
- return different authority outcomes when the underlying facts change;
- approve when the required authority conditions are satisfied;
- refuse when the actor, role, authority scope, or required authority condition does not satisfy the configured posture;
- preserve an original refusal when a later authorized supervised path changes the final outcome;
- produce reviewable decision evidence for the governed outcome;
- show alignment between the governed decision and downstream handling where that evidence is included;
- reject a direct attempt outside the required governed path in the configured demo workflow.

In plain English:

The tests show that SEAL can make an authority decision before the scoped filing path proceeds — and leave evidence of what it decided.

What This Packet Does Not Prove

This packet does **not** prove:

- that any law firm's policy or authority model is legally correct;
- that a filing is legally sufficient, strategically wise, ethical, or appropriate in a particular jurisdiction;
- that upstream identity, matter, consent, or other source data is accurate;
- that every workflow or execution path in a buyer environment is governed;
- production non-bypassability inside a future customer environment;
- buyer-specific security, integration, availability, or production readiness;
- that a refusal prevented malpractice, financial loss, legal harm, or another downstream consequence;
- that SEAL replaces lawyer judgment, professional supervision, court rules, IAM, GRC, matter systems, DMS, filing tools, or other firm controls;
- that any buyer has deployed SEAL in production.

Why That Boundary Matters

A serious proof packet should make clear **where the evidence stops**.

These exhibits are not a claim that SEAL governs an entire firm. They **are not** a certification of legal correctness. They **are not** a substitute for customer-specific security, workflow, authority, or production diligence.

They demonstrate a narrower thing:

For the scoped evaluator workflow, the authority control behaved as shown, and the resulting decision evidence can be reviewed.

The tests use **synthetic, evaluator-controlled scenarios** and public redactions. Customer production deployment requires separate scoping, authority mapping, integration review, security review, continuity review, and written agreement.

The packet proves the control behavior shown here. It does not prove the world around the control.

What Existing Controls Already Govern — and the Question That Can Remain at Final Submit

Most firms already have important controls around legal work: identity systems, GRC, matter systems, document systems, filing tools, workflow tools, AI gateways, and audit logs.

Those controls matter. They answer important questions about identity, policy, matter context, documents, workflow, and activity.

SEAL evaluates one narrower question at final submit:

Before the filing leaves the firm, is this actor authorized to take this action, in this matter, under this authority, with the required evidence?

That is the Commit Layer: the pre-execution authority gate before the institution is committed.

Existing control	What it establishes	What may remain unanswered	The final-submit authority question
IAM / SSO	Who can access systems	Whether this identity has authority for this specific filing/action.	Valid login is not valid authority to bind
GRC / policy	Written rules, control ownership, audit posture	Whether the applicable policy becomes an inline authority decision at final submit.	Policy must become a runtime verdict
Matter system	Matter, client, workflow context	Whether matter and workflow context are connected to authority for this specific action.	Context must connect to authority before action
DMS	Document access, versioning, storage	Whether document access establishes authority to take the external action.	The risk is often the commitment, not the document
Filing / workflow tools	Local process steps and submission state	Whether this actor has matter/action-specific authority at final submit	Applies the scoped authority decision in the governed path
AI gateway	AI interaction, prompt/output/model -call governance	Whether AI interaction governance establishes authority for the specific institutional action.	Safe output can still drive unauthorized action
Audit / logging	What happened after the fact	Whether an authority decision occurred before execution.	A record after the fact is not a pre-commit authority decision.
SEAL Legal Runtime at the Commit Layer	Runtime approve / refuse / supervised override	Whether this final-submit path is within the configured governed scope.	Provides an authority decision before the firm is committed

Existing systems govern around the action. The Commit Layer governs the action boundary itself.

What SEAL Governs

SEAL governs one narrow question before a filing leaves the firm:

Is this actor authorized to take this action, in this matter, under this authority?

The firm's existing systems remain the sources of truth for governance facts such as identity, role, matter context, authority, consent, and supervision.

SEAL does not decide whether the filing is legally correct, strategically wise, or appropriate for the matter.

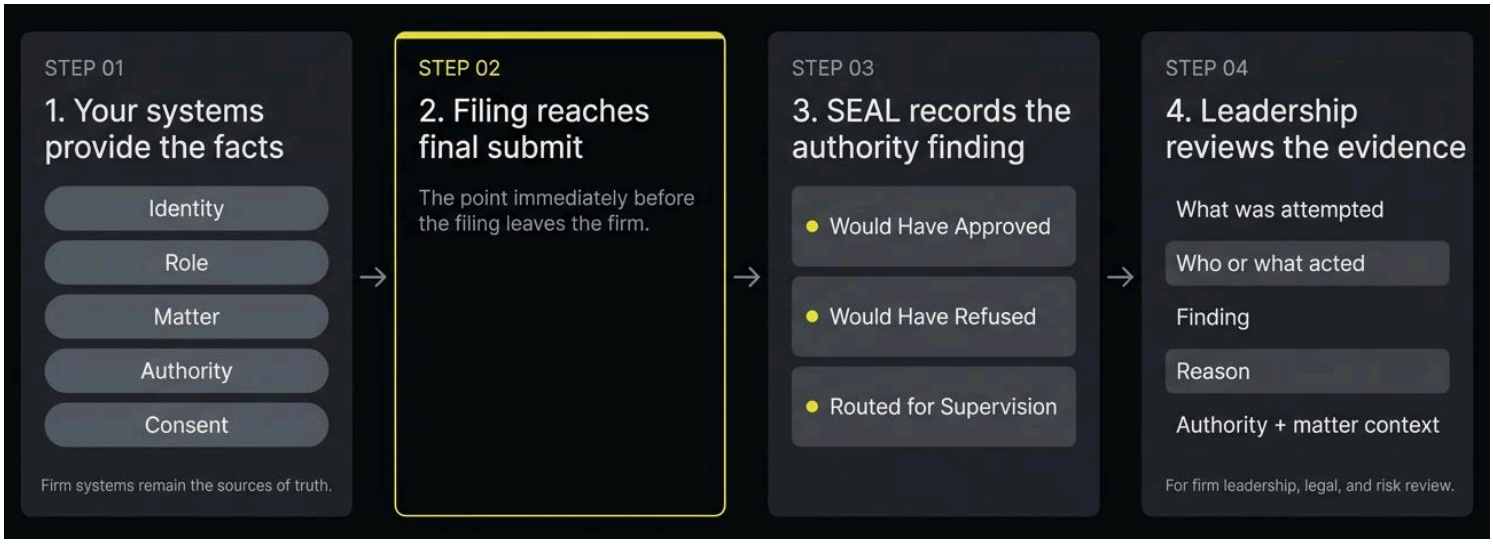
For the scoped workflow, SEAL evaluates the authority question before the filing leaves the firm against the authority conditions and returns a governed outcome:

Approved / Refused / Routed for Supervision

When a required authority condition is missing or unresolved,
SEAL does not silently turn that uncertainty into approval.

Each governed outcome produces a reviewable decision record showing what the control decided at the moment of action.

In plain English: SEAL governs whether the action may proceed under the firm's configured authority conditions — not the substance of the legal work.



Who Owns What

The Firm Owns

- legal judgment and professional supervision
- policies and authority rules
- identity and role sources
- matter and workflow context
- who may supervise or approve exceptions
- workflow routing and escalation
- retention, use, and disclosure of its decision records
- whether a workflow remains observe-only or later moves into controlled enforcement

Thinking OS™ Is Responsible For

- operating SEAL Legal Runtime within the agreed scope
- returning governed outcomes for the scoped workflow
- producing reviewable decision records
- maintaining the runtime's security, integrity, and availability posture within agreed scope
- supporting the agreed evaluation or integration path

The firm defines the authority model.

SEAL evaluates the governed action against that configured authority posture.

> **The firm owns the rules and legal judgment. Thinking OS™ operates the runtime.**

What SEAL Does Not Do

SEAL Legal Runtime is a **pre-execution authority gate for governed legal actions.**

It evaluates whether the configured authority conditions for the scoped action are satisfied and produces reviewable decision evidence.

It does **not**:

- draft, edit, sign, send, or file legal documents
- provide legal advice
- choose litigation strategy
- decide whether a filing is legally correct or strategically wise
- replace lawyers, supervisors, or professional judgment
- replace GRC, IAM, matter systems, DMS, filing tools, or workflow systems
- become the system of record for the matter or filing
- invent the firm's policies, roles, authority, or supervision model
- govern workflows that are not in the agreed wired scope

SEAL can refuse. It cannot file.

An approval means the configured governance conditions for the scoped action were satisfied.

It does **not** certify legal merits, strategy, ethics, professional judgment, or jurisdictional correctness.

The firm remains responsible for the legal action and what happens next.

Scenario 1 — Authorized Filing

The required authority conditions were satisfied

This test asks the simplest question:

> **What happens when the actor is authorized and the required conditions for the filing are present?**

What happened?

A synthetic, evaluator-controlled filing request was submitted for an **Administrative Law / Motion to Extend Time** workflow.

For this test:

- the actor was recognized as an authorized attorney;
- the required authority conditions were present;
- consent was present;
- the filing request matched the configured workflow and matter context.

What did SEAL decide?

Approve.

Why?

The governed request satisfied the configured authority conditions for that filing action.

SEAL did not approve the legal merits of the filing.

It approved the **authority to take the governed action under the configured conditions.**

Did the action bind?

Not established by this evaluator test.

After SEAL returned approval, it sent the approved request to the configured receiving system. The receiving system returned a successful response to SEAL's handoff request.

It does not establish that the filing was recorded, docketed, accepted by an institution, or given legal or institutional effect. This confirms handoff-level success only.

approved → downstream handoff attempted → receiving system returned success

What happens next?

The firm still owns the legal action.

SEAL does not decide whether the filing is legally correct, strategically wise, ethically appropriate, or ready for submission.

Lawyers and supervisors remain responsible for legal judgment, professional supervision, and the filing itself.

Where is the evidence?

The technical exhibits later in this packet show:

- the SEAL-generated approval artifact;
- the governed approval outcome;
- runtime / enforcement posture
- downstream handoff result
- external-effect boundary shown in the artifact
- alignment between the governed decision and downstream handoff
- redacted evidence-anchor categories supporting later review.

Bottom line: *when the required authority conditions were satisfied, SEAL approved the action before the filing path proceeded and left decision evidence.*

Test posture: Synthetic, evaluator-controlled. Public redactions applied. This is not a customer production deployment.

Scenario 2 — Wrong Authority

The authority existed — but it belonged to a different matter

This test asks:

> **What happens when an attorney attempts a filing, but the signed authority is scoped to a different matter?**

What happened?

A synthetic, evaluator-controlled filing request was submitted for an Administrative Law / Motion to Extend Time workflow.

The actor resolved to **Attorney**.

Signed authority was present. The filing action, docket, and legal workflow context were aligned with the governed request.

But the signed authority identified a **different matter** from the matter the filing request was attempting to act on.

What did SEAL decide?

Refuse — SEAL-AUTH-SCOPE.

Why?

The signed authority scope did not match the requested matter scope.

The important distinction is simple:

Having authority is not enough. It must be authority for this matter.

Did the action bind?

No — in this controlled evaluator test.

SEAL returned refusal before execution. The configured executor handoff was not attempted.

What happens next?

The firm owns the next valid path.

A future governed submission may include corrected authority evidence whose scope matches the requested matter, docket, filing action, and legal workflow context.

SEAL does not create that authority, decide whether it should be granted, or determine whether the filing should ultimately be made.

It records the governed authority decision.

Where is the evidence?

The technical exhibit later in this packet shows:

- the **SEAL-AUTH-SCOPE** refusal;
- the requested matter scope;
- the signed-authority matter scope;
- the recorded mismatch type: **matter**;
- the refusal before executor handoff; and
- redacted decision and evidence-anchor categories supporting later review.

Bottom line: *the actor had signed authority, but not authority for this matter. SEAL refused the action before the scoped filing path proceeded.*

Test posture: Synthetic, evaluator-controlled. Public redactions applied. This is not a customer production deployment.

Scenario 3 — Role Not Permitted

The actor was known, but the role was not allowed to take this filing action

This test asks:

> **What happens when SEAL knows who the actor is, but that actor's role is not permitted to take the governed action?**

What happened?

A synthetic, evaluator-controlled legal action was submitted for an **Administrative Law / Motion to Compel Production** workflow.

The actor's identity and group context were recognized.

The acting role resolved to **Paralegal**.

Under the configured authority rules for this workflow, that role was **not permitted to take the governed filing action**.

What did SEAL decide?

Refuse.

Why?

The problem was not missing identity.

SEAL knew who the actor was and which role applied.

The refusal occurred because the **recognized role itself was not authorized for that specific action**.

The distinction is important:

> **Knowing who someone is does not mean they are authorized to do everything the system can reach.**

Did the action bind?

No — in this controlled evaluator test.

SEAL returned refusal before the configured filing path proceeded.

What happens next?

The firm owns the next valid path.

That may mean routing the matter to an authorized lawyer, correcting the workflow, or following another firm-defined supervision or remediation process.

SEAL does not choose the lawyer, decide whether the filing should be made, or replace professional supervision.

It records the authority decision.

Where is the evidence?

The technical exhibit later in this packet shows:

- the SEAL refusal outcome;
- the role-based refusal reason;
- the trusted actor and role context;
- the relevant policy reference;
- redacted decision and evidence-anchor categories supporting later review.

Bottom line: *the actor was known, but the role was not permitted to take this filing action. SEAL refused the action before the scoped path proceeded.*

Test posture: Synthetic, evaluator-controlled. Public redactions applied. This is not a customer production deployment.

Scenario 4 — Required Consent Missing

The actor and filing context were otherwise in scope, but a required authority condition was missing

This test asks:

> **What happens when the actor and filing context are acceptable, but a required consent or authority condition has not been satisfied?**

What happened?

A synthetic, evaluator-controlled filing request was submitted for an **Administrative Law / Motion to Extend Time** workflow.

For this test:

- the actor was recognized;
- the filing type matched the configured workflow;
- a required consent condition was not satisfied at the time of action.

What did SEAL decide?

Refuse.

Why?

The governed filing required consent as part of the configured authority posture.

That condition was missing.

The distinction is important:

A filing can look otherwise valid and still lack the authority required to proceed.

SEAL did not treat the missing condition as a warning or something to reconstruct later.

It returned a governed refusal for the scoped action.

Did the action bind?

No — in this controlled evaluator test.

SEAL returned refusal before the configured filing path proceeded.

What happens next?

The firm owns the next valid path.

That may mean obtaining the required consent, correcting the authority context, routing the matter for supervision, or following another firm-defined remediation process.

SEAL does not decide whether consent should be given or whether the filing should ultimately proceed.

It records whether the configured authority condition was satisfied at the moment of action.

Where is the evidence?

The technical exhibit later in this packet shows:

- the SEAL refusal outcome;
- the missing-consent reason category;
- the relevant policy and authority context;
- the decision-reference and evidence-anchor categories preserved for later review.

Bottom line: *the actor and filing context were otherwise in scope, but the required consent condition was missing. SEAL refused the action before the scoped filing path proceeded.*

Test posture: Synthetic, evaluator-controlled. Public redactions applied. This is not a customer production deployment.

Scenario 5 — Authorized Supervised Path

The original refusal stayed on the record, and the action changed only through authorized supervision

This test asks:

What happens when SEAL refuses an action, but the firm has a valid supervised path for an authorized person to review and approve the exception?

What happened?

A synthetic, evaluator-controlled filing request for an Administrative Law / Motion for Summary Judgment reached the final-submit authority check.

The initial actor resolved to a **paralegal role that was not permitted to take the governed filing action.**

SEAL recorded the baseline governance decision:

Refuse — SEAL-ROLE-DISALLOWED

A supervising partner then used the configured supervised path with the required authority evidence, bound to the refused parent decision.

What did SEAL decide?

The **original refusal remained recorded**.

The final outcome changed only after the configured supervised path was satisfied.

The resulting record shows:

- the baseline refusal;
- the supervising authority;
- required signed authority recorded;
- linkage to the refused parent decision; and
- a final **supervised override — approved** outcome.

This was not treated as an ordinary approval.

Why?

The point of supervision is not to erase the original “no.”

It is to provide a separately governed path for an authorized person to take responsibility for the exception.

> **Supervision is not a silent bypass. The refusal remains visible, and the later authorized decision is recorded separately.**

Did the action bind?

Not established by this evaluator test.

After the authorized supervised path was satisfied, SEAL sent the governed request to the configured receiving system.

The receiving system returned a successful response to SEAL’s handoff request.

This establishes **handoff-level success only.** It does not establish that the filing was recorded, docketed, accepted by an institution, or given legal or institutional effect.

What happens next?

The firm remains responsible for the supervisory decision and the legal action.

SEAL does not decide whether an exception should be granted as a matter of legal strategy or professional judgment.

The firm decides who may supervise, what authority is required, and whether the exception should be used.

SEAL records the governed path and its outcome.

Where is the evidence?

The technical exhibits later in this packet show:

- the original refusal and refusal code;
- the supervising authority record;
- the supervised-override outcome;
- linkage between the override and the refused parent decision;
- required signed authority recorded;
- the final governed outcome;
- the downstream handoff result; and
- the external-effect boundary.

Bottom line: *SEAL preserved the original refusal. The outcome changed only through a separately governed supervisory decision with authority recorded and linked to the refused parent decision. The configured receiver then returned success to SEAL's handoff request; external institutional effect was not confirmed.*

What the Scenarios Show Together

The five scenarios test the same narrow authority question under different facts:

> **Is this actor authorized to take this action, in this matter, under this authority, before the filing path proceeds?**

The answer changed when the facts changed.

When the required authority conditions were satisfied

- **SEAL approved the action.**
- The configured filing path was allowed to proceed, and reviewable decision evidence was produced.

When signed authority existed but belonged to the wrong matter

- **SEAL refused the action.**
- The authority had to match the specific matter the governed filing request was attempting to act on.

When the actor was known but the role was not permitted

- **SEAL refused the action.**
- Identity was not the problem. The recognized role itself was not authorized for that governed action.

When required consent was missing

- **SEAL refused the action.**
- The filing context could otherwise be acceptable while still lacking a required authority condition.

When an authorized supervisory path was used

- **The original refusal remained on the record.**
- The final outcome changed only through a separately governed supervisory decision with authority recorded.

The Common Pattern

Across all five tests:

- **the firm-defined authority conditions controlled the decision**
- **SEAL returned an explicit governed outcome**
- **the decision occurred before the scoped filing path proceeded**
- **the firm retained legal judgment and supervision**
- **each governed outcome left reviewable decision evidence**

The tests do not show that SEAL decides whether legal work is correct.

They show something narrower:

> **SEAL can distinguish between authorized, unauthorized, and supervision-required filing actions before the scoped path proceeds — and preserve evidence of the decision.**

These are **synthetic, evaluator-controlled tests**, not customer production deployments.

Technical Evidence Begins Here

For Technical Evaluators, Risk, Procurement, Insurers, and Other Qualified Reviewers

The preceding pages explain the five evaluator scenarios in plain English.

The pages that follow contain the **underlying technical evidence supporting those summaries.**

This section is intentionally more detailed.

It includes the actual redacted Layer 1 Decision Records, Layer 2 review evidence, runtime outcomes, execution records, evidence references, and configured-path tests used to examine the scoped control behavior.

How to Read This Section

For each exhibit, the evaluator should be able to connect five things:

1. What action was attempted?
The governed legal action and relevant context.

2. What did SEAL decide?
Approved, Refused, or Approved Through Supervised Override.

3. What runtime and downstream handling occurred?
Whether the runtime was observe-only or enforcing, whether a downstream handoff was attempted, and what result the configured receiving system returned.

4. What external effect, if any, was established?
Whether the evidence establishes no downstream action, handoff-level success, or a separately confirmed external institutional effect.

5. What evidence remains?
The decision record, trace or decision references, authority and policy context, and supported integrity evidence available for review.

The technical fields exist to support those questions.

They are not separate claims from the plain-English scenarios.

What This Evidence Is Intended to Demonstrate

For the scoped evaluator workflow, the exhibits are designed to let a qualified reviewer inspect:

- governed approval evidence;
- governed refusal evidence across different refusal conditions;
- an authorized supervised path that preserves the original refusal;
- the relationship between governance decisions and downstream handling where demonstrated;
- reviewable decision records and supporting references;
- configured demo-path behavior where a valid governed outcome is required.

Evaluation Boundary

These exhibits come from **synthetic, evaluator-controlled tests** and are shown with public redactions.

They demonstrate the scoped behavior shown in this packet.

They do **not** establish:

- buyer-specific production readiness;
- production non-bypassability in a future customer environment;
- correctness of a law firm's legal or policy judgment;
- universal coverage across unwired workflows;
- replacement of security, integration, operational, or legal diligence.

Public redactions remove sensitive implementation, routing, identity, infrastructure, and other non-public details while preserving the evidence needed to evaluate the stated control behavior.

> **The plain-English scenario section tells you what happened. This section shows the evidence behind it.**

Approval Evidence

Note:

Where an approval or supervised-path exhibit shows a successful downstream receipt, that receipt establishes handoff-level success only. External recording, docketing, institutional acceptance, or legal effect is not established unless separately shown.

Evaluator View — Approval Decision Record

SEAL-generated Layer 1 Decision Record from a synthetic, evaluator-controlled request, shown with public redactions. This view shows the approval outcome, enforcement posture, downstream handoff result, external-effect boundary, what was approved or attempted, the control reason, post-approval handoff, and redacted evidence anchors. The narrow proof point: under the configured evaluator conditions, approval was recorded before the configured downstream handoff proceeded.

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance and runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Approved

APPROVAL CODE
SEAL-APP-ALLOWED-001

2. Runtime Posture

RUNTIME MODE
Enforce

RUNTIME SUMMARY
Enforce (runtime decisions are applied in-line with governance policy).

FINAL RUNTIME DECISION
approval

DECISION ALIGNMENT
Aligned

EXECUTION / HANDOFF
Successful response to handoff request

3. SEAL Enforced?

SEAL ENFORCED?
Yes

ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL / EXTERNAL EFFECT
Configured receiving system returned a successful response to SEAL's handoff request; external effect not confirmed

Governance approval, runtime approval, configured receiving-system handoff, artifact persistence, and notification delivery are not institutional effect proof. External effect is confirmed only when upstream external_commit truth and a bounded receipt establish it.

5. What Was Approved / Attempted

ACTION
Motion to Extend Time

ACTOR
[redacted]

ROLE
Attorney

MATTER ID
[redacted]

DOCKET ID
[redacted]

FINAL-SUBMIT TARGET / DESTINATION
Agency Filing Portal

Approval Evidence Continued Below

6. Why

Governance approved this action because supplied identity, scope, and authority/evidence controls were reported satisfied. The configured receiving system returned a successful response to SEAL's handoff request; external effect is not confirmed by this record.

7. Next Valid Path / Post-Approval Handoff

POST-APPROVAL HANDOFF

Execution handoff receipt recorded at SEAL's configured handoff seam.

The firm owns post-approval recordkeeping, review, retention, downstream workflow, and later institutional disposition unless an explicit upstream contract says otherwise. External or institutional effect is governed by the Binding / Institutional Effect field above and must not be inferred from this handoff row.

8. Evidence Anchors

DECISION ID

[redacted]

ARTIFACT ID

[redacted]

AUDIT TRACE ID

[redacted]

POLICY / VERSION

[redacted]

TIMESTAMP

[redacted]

Layer 2 — Downstream Handoff: Approval, Enforce Posture, Successful Response, Aligned

Layer 2 — Review Evidence: Governance vs Runtime

Supplied governance, runtime, execution, and executor-gate facts for review. This record does not determine legal merits, infer execution success, infer gate status, or establish institutional effect.

Runtime Decision Path

Governance, runtime posture, pre-execution runtime, final runtime, and alignment facts supplied by upstream governance/runtime layers.

Governance Decision	approval
Pre-Execution Runtime Decision	approval
Final Runtime Decision	approval
Decision Alignment	aligned

Execution Receipt

Receipt-only execution metadata supplied to this record. The record does not call or operate downstream systems.

Status	ok
Attempted	True
OK	True
Required	True
Effective Enforcement	True
Execution Outcome	succeeded
Execution Receipt Alignment	aligned
Blocks Effective Completion	False
Control Meaning	SEAL approved this request under the firm's rules and sent it to the required firm-configured receiving system. The configured receiving system returned a successful HTTP response to SEAL's handoff request. This confirms handoff-level success only. It does not prove that the governed action was recorded, completed, docketed, accepted by an institution, or given legal or institutional effect.

Control meaning

Plain-language runtime/control meaning supplied by upstream runtime or governance metadata when present.

Plain-Language Control Meaning	SEAL approved this request under the firm's rules and sent it to the required firm-configured receiving system. The configured receiving system returned a successful HTTP response to SEAL's handoff request. This confirms handoff-level success only. It does not prove that the governed action was recorded, completed, docketed, accepted by an institution, or given legal or institutional effect.

This Layer 2 execution view confirms the approval did not remain a policy note or dashboard event. The governance decision, final runtime decision, and downstream handoff evidence tell the same control story: approved, enforce posture, handoff attempted, successful response, aligned. ***This confirms handoff-level success only. External institutional effect is not established by this exhibit.*** *Public redactions remove endpoint, routing, and infrastructure details while preserving evaluator-visible proof of controlled execution.*

How to Read This Approval Decision Record

This Decision Record should be read as evidence of runtime authority control, not legal judgment. SEAL did not decide whether the filing was strategically wise, legally sufficient, or jurisdictionally correct. It evaluated whether configured authority conditions were satisfied before the filing path proceeded.

Approval is not the absence of governance. It is a governed authority decision made before the configured downstream action proceeds.

What to verify

1. **Governed request —** the filing-path action was presented to SEAL before execution.
2. **Approval outcome** — SEAL returned approval under the configured authority posture.
3. **Runtime alignment** — the governance decision and runtime decision matched.
4. **Downstream handoff** — after governed approval, the configured receiving system returned a successful response to SEAL's handoff request.
5. **External-effect boundary** — the exhibit does not claim that the filing was recorded, docketed, accepted by an institution, or given legal effect.
6. **Evidence surface** — reviewable evidence-anchor categories remain visible, with sensitive values redacted.

Wrong-Authority Refusal Evidence

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance/runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Refused

REFUSAL CODE
SEAL-AUTH-SCOPE

2. Runtime Posture

RUNTIME MODE
Enforce

RUNTIME SUMMARY
Enforce (runtime refusals are applied in-line with governance policy).

FINAL RUNTIME DECISION
refusal

DECISION ALIGNMENT
aligned

3. SEAL Enforced?

SEAL ENFORCED?
Yes

ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL EFFECT
No

Execution handoff, artifact persistence, notification delivery, or governance refusal alone is not institutional effect proof. External effect requires a confirmed upstream external_commit plus a bounded receipt; otherwise this record says not established.

Wrong-Authority Refusal Evidence Continued Below

5. What Was Attempted

ACTION
Motion To Extend Time

ACTOR
[redacted]

TRUSTED / RESOLVED ROLE
Attorney

MATTER ID
[redacted]

DOCKET ID
[redacted]

FINAL-SUBMIT TARGET / DESTINATION
Agency Filing Portal

6. Why

Governance refused this action because the signed authority scope did not match the requested matter scope.

7. Next Valid Path

NEXT VALID PATH
Future governed submission may include corrected authority evidence

OWNER
Tenant owned authority or governance owner

REQUIRED
3 supplied required inputs; full details preserved in Layer 2 / Next Steps.

SOURCE
SEAL neutral default

SEAL records the governed next path; the firm owns remediation, review, escalation, recordkeeping, and workflow.

8. Evidence Anchors

DECISION ID
[redacted]

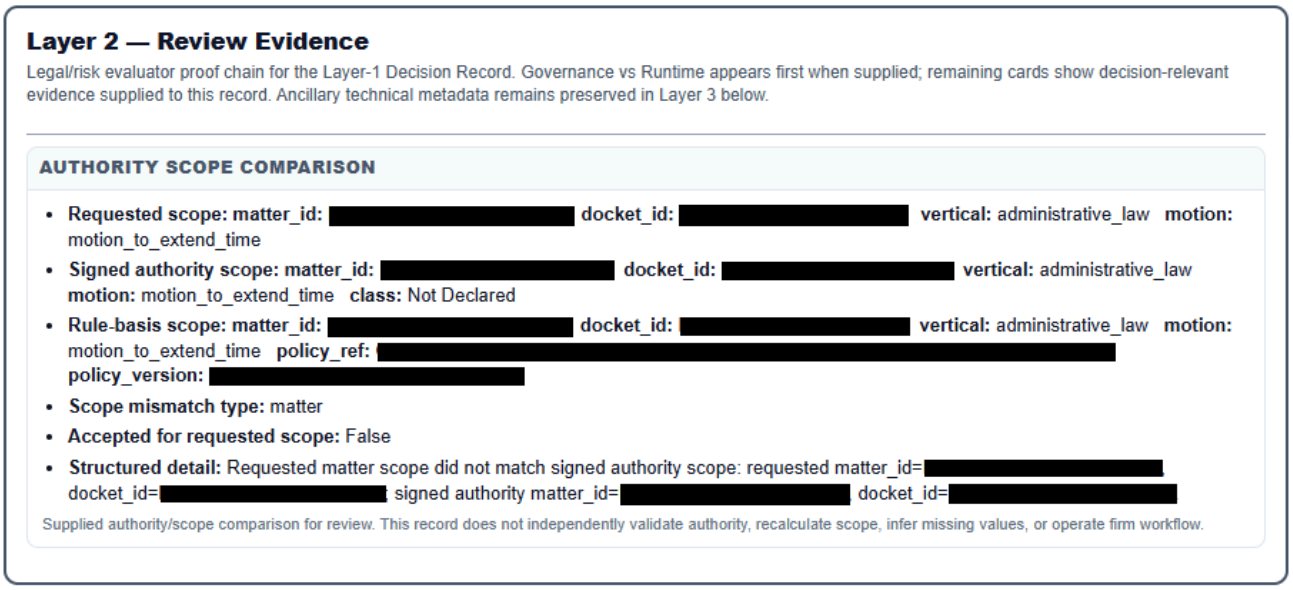
ARTIFACT ID
[redacted]

AUDIT TRACE ID
[redacted]

POLICY / VERSION
[redacted]

TIMESTAMP
[redacted]

Authority Scope Comparison — Requested Matter vs. Signed Authority Matter.



Layer 2 — Review Evidence

Legal/risk evaluator proof chain for the Layer-1 Decision Record. Governance vs Runtime appears first when supplied; remaining cards show decision-relevant evidence supplied to this record. Ancillary technical metadata remains preserved in Layer 3 below.

AUTHORITY SCOPE COMPARISON

- **Requested scope: matter_id:** [redacted] **docket_id:** [redacted] **vertical:** administrative_law **motion:** motion_to_extend_time
- **Signed authority scope: matter_id:** [redacted] **docket_id:** [redacted] **vertical:** administrative_law **motion:** motion_to_extend_time **class:** Not Declared
- **Rule-basis scope: matter_id:** [redacted] **docket_id:** [redacted] **vertical:** administrative_law **motion:** motion_to_extend_time **policy_ref:** [redacted] **policy_version:** [redacted]
- **Scope mismatch type:** matter
- **Accepted for requested scope:** False
- **Structured detail:** Requested matter scope did not match signed authority scope: requested matter_id=[redacted] docket_id=[redacted] signed authority matter_id=[redacted] docket_id=[redacted]

Supplied authority/scope comparison for review. This record does not independently validate authority, recalculate scope, infer missing values, or operate firm workflow.

Scenario

A governed filing request was evaluated under the Enforce runtime posture for **Administrative Law / Motion To Extend Time.**

The actor resolved to **Attorney**, and signed authority was present.

The requested filing and the signed authority matched on the docket, filing action, and legal environment — but the signed authority was scoped to a **different matter**.

What SEAL returned

SEAL returned a governed refusal with code **SEAL-AUTH-SCOPE**.

The runtime recorded:

Finding / Decision — Refused
Runtime Mode — Enforce
SEAL Enforced — Yes
Institutional Effect — No
Executor Handoff — Not attempted after refusal

The resulting terminal artifact was fetched and its published V1 artifact hash verified in the evaluator run.

Why it matters

This tests a different control problem from role permission.

The actor was not unknown or structurally disallowed. Signed authority existed.

The issue was **scope**: the authority did not belong to the matter the governed action was attempting to affect.

Bottom line

Authority is not portable across matters.

SEAL refused because the signed authority did not match the requested matter before the scoped filing path proceeded.

Generated from a synthetic, evaluator-controlled request and redacted for public review. Control outcome and evidence-reference categories are preserved; sensitive values, routing details, operational contacts, and live destinations are redacted.

Role-Not-Permitted Refusal Evidence

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance/runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Refused

REFUSAL CODE
SEAL-ROLE-DISALLOWED

2. Runtime Posture

RUNTIME MODE
Enforce

RUNTIME SUMMARY
Enforce (runtime refusals are applied in-line with governance policy).

FINAL RUNTIME DECISION
refusal

DECISION ALIGNMENT
aligned

3. SEAL Enforced?

SEAL ENFORCED?
Yes

ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL EFFECT
No

Execution handoff, artifact persistence, notification delivery, or governance refusal alone is not institutional effect proof. External effect requires a confirmed upstream external_commit plus a bounded receipt; otherwise this record says not established.

5. What Was Attempted

ACTION
Motion To Compel Production

ACTOR
[redacted]

TRUSTED / RESOLVED ROLE
Paralegal

MATTER ID
[redacted]

DOCKET ID
[redacted]

FINAL-SUBMIT TARGET / DESTINATION
Internal System

Role-Not-Permitted Refusal Evidence Continued Below

6. Why

Governance refused this action because Role 'Paralegal' is explicitly disallowed under the Administrative Law vertical policy.

7. Next Valid Path

NEXT VALID PATH
Future governed submission may include authorized role or firm owned review metadata

OWNER
Tenant identity role mapping or supervisory review owner

REQUIRED
4 supplied required inputs; full details preserved in Layer 2 / Next Steps.

SOURCE
SEAL neutral default

SEAL records the governed next path; the firm owns remediation, review, escalation, recordkeeping, and workflow.

8. Evidence Anchors

DECISION ID
[redacted]

ARTIFACT ID
[redacted]

AUDIT TRACE ID
[redacted]

POLICY / VERSION
[redacted]

TIMESTAMP
[redacted]

Scenario

A governed legal action was evaluated under the Enforce runtime posture for **Administrative Law / Motion To Compel Production**. The trusted role resolved to **Paralegal** from the supplied identity and role context.

What SEAL returned

SEAL returned a governed refusal with code **SEAL-ROLE-DISALLOWED**. Layer 1 records the enforced refusal, trusted role, attempted action, control reason, next valid path, and redacted evidence anchors. Detailed review evidence and technical verification remain preserved in the underlying record.

Why it matters

Under the configured evaluator conditions, this shows that refusal is not limited to unknown identity or missing mapping. Even when the identity is known and the trusted role is resolved, **SEAL can refuse when that role is not permitted for the configured action.**

Caption

This exhibit shows a governed refusal recorded before the configured downstream path proceeded. Layer 1 shows what was **attempted, the trusted role, the enforcement posture, why the action was refused, the next valid path,** and **the categories of evidence anchors** preserved for review.

Generated from a synthetic, evaluator-controlled request and redacted for public review. Control outcome and evidence-reference categories are preserved; sensitive values, routing details, operational contacts, and live destinations are redacted.

Missing-Consent Refusal Evidence

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance/runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Refused

REFUSAL CODE
SEAL-CONSENT-001

2. Runtime Posture

RUNTIME MODE
Enforce

RUNTIME SUMMARY
Enforce (runtime refusals are applied in-line with governance policy).

FINAL RUNTIME DECISION
refusal

DECISION ALIGNMENT
aligned

3. SEAL Enforced?

SEAL ENFORCED?
Yes

ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL EFFECT
No

Execution handoff, artifact persistence, notification delivery, or governance refusal alone is not institutional effect proof. External effect requires a confirmed upstream external_commit plus a bounded receipt; otherwise this record says not established.

5. What Was Attempted

ACTION
Motion To Extend Time

ACTOR
[redacted]

TRUSTED / RESOLVED ROLE
Attorney

MATTER ID
[redacted]

DOCKET ID
[redacted]

FINAL-SUBMIT TARGET / DESTINATION
Internal System

Missing-Consent Refusal Evidence Continued Below

6. Why

Governance refused this action because No valid client consent record or consent token-of-record was declared for this matter and motion.

7. Next Valid Path

NEXT VALID PATH
Attach consent record or token for governed resubmission

OWNER
Tenant owned matter team or consent system

REQUIRED
3 supplied required inputs; full details preserved in Layer 2 / Next Steps.

SOURCE
SEAL neutral default

SEAL records the governed next path; the firm owns remediation, review, escalation, recordkeeping, and workflow.

8. Evidence Anchors

DECISION ID
[redacted]

ARTIFACT ID
[redacted]

AUDIT TRACE ID
[redacted]

POLICY / VERSION
[redacted]

TIMESTAMP
[redacted]

Scenario

A governed filing request was evaluated under the Enforce runtime posture for **Administrative Law / Motion To Extend Time**. The trusted role resolved to Attorney, but no valid client consent record or consent token-of-record was declared for the matter and motion.

What SEAL returned

SEAL returned a governed refusal with code **SEAL-CONSENT-001**. Layer 1 records the enforced refusal, attempted action, trusted role, consent-related control reason, tenant-owned next valid path, and redacted evidence anchors. Detailed review evidence and technical verification remain preserved in the underlying record.

Why it matters

Under the configured evaluator conditions, this shows that refusal is not limited to role or authority-scope failures. SEAL also refused when a required consent condition was not satisfied before the configured downstream path proceeded.

Caption

This exhibit shows a governed refusal recorded before the configured downstream path proceeded. Layer 1 shows what was attempted, the trusted role, the enforcement posture, why the consent condition failed, the tenant-owned next valid path, and the categories of evidence anchors preserved for review.

Generated from a synthetic, evaluator-controlled request and redacted for public review. Control outcome and evidence-reference categories are preserved; sensitive values, routing details, operational contacts, and live destinations are redacted.

Authorized Supervised Path Evidence

Evaluator View — Supervised Override Decision Record

SEAL-generated runtime artifact from a synthetic, evaluator-controlled Motion for Summary Judgment request, shown with public redactions.

The initial final-submit attempt received a baseline refusal because the actor's role was not permitted for the governed action. A supervising partner then used the configured supervised path with required authority recorded and linked to the refused parent decision.

The final governed outcome was Approved Through Supervised Override. The configured receiving system subsequently returned a successful response to SEAL's handoff request.

That establishes handoff-level success only. External institutional effect is not established by this exhibit.

Note:

Where an approval or supervised-path exhibit shows a successful downstream receipt, that receipt establishes handoff-level success only. External recording, docketing, institutional acceptance, or legal effect is not established unless separately shown.

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance and runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Approved Through Supervised Override
APPROVAL CODE
SEAL-OVERRIDE-APPROVED

2. Runtime Posture

RUNTIME MODE
Enforce
RUNTIME SUMMARY
Enforce (runtime decisions are applied in-line with governance policy).
FINAL RUNTIME DECISION
approval
DECISION ALIGNMENT
Diverged
EXECUTION / HANDOFF
Successful response to handoff request

3. SEAL Enforced?

SEAL ENFORCED?
Yes
ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL / EXTERNAL EFFECT
Configured receiving system returned a successful response to SEAL's handoff request; external effect not confirmed

Governance approval, runtime approval, configured receiving-system handoff, artifact persistence, and notification delivery are not institutional effect proof. External effect is confirmed only when upstream external_commit truth and a bounded receipt establish it.

5. What Was Approved / Attempted

ACTION
Motion for Summary Judgment
ACTOR
[redacted]
ROLE
Partner
MATTER ID
[redacted]
DOCKET ID
[redacted]
FINAL-SUBMIT TARGET / DESTINATION
Internal System

Authorized Supervised Path Evidence Continued Below

6. Why

Governance approved this action through a supervised override of the baseline SEAL-ROLE-DISALLOWED refusal. Parent decision anchor, override actor, and signed-authority recording are preserved in Decision Lineage and the Formal Override Path. The configured receiving system returned a successful response to SEAL's handoff request; external effect is not confirmed by this record.

7. Next Valid Path / Post-Approval Handoff

POST-APPROVAL HANDOFF

Execution handoff receipt recorded at SEAL's configured handoff seam.

The firm owns post-approval recordkeeping, review, retention, downstream workflow, and later institutional disposition unless an explicit upstream contract says otherwise. External or institutional effect is governed by the Binding / Institutional Effect field above and must not be inferred from this handoff row.

8. Evidence Anchors

DECISION ID [redacted]

ARTIFACT ID [redacted]

AUDIT TRACE ID [redacted]

POLICY / VERSION [redacted]

TIMESTAMP [redacted]

9. Decision Lineage

PARENT REFUSAL

SEAL-ROLE-DISALLOWED • Parent decision: [redacted]

OVERRIDE ACTOR

[redacted] (role=partner, [redacted])

AUTHORITY RECORDED

Yes

SIGNED AUTHORITY REQUIRED

Yes

SIGNED AUTHORITY RECORDED

Yes

BOUND TO PARENT DECISION

Yes (upstream parent reference supplied)

OUTCOME

Approved through supervised override

This is a compact display of the upstream override_contract. The detailed Formal Override Path record remains preserved below.

Outcome — Supervised Override: Refusal Preserved, Authority Recorded

Formal Override Path

Upstream-supplied override_contract capsule preserving override outcome, parent linkage, actor, authority/callback, and signed-authority recording facts. This record does not validate override authority, approve, override, create tickets, or operate tenant workflow.

Override contract outcome

Upstream-supplied override_contract envelope and terminal override outcome.

Override Attempted	true
Override Outcome	approved

Refused-parent linkage

Parent and baseline decision references echoed from the override contract. This notifier does not validate linkage.

Baseline Refusal Code	SEAL-ROLE-DISALLOWED

Authority and actor record

Authority, reviewer, and override-actor metadata echoed as supplied. Current reviewer is not substituted as override actor.

Override Kind	supervised_override
Override Actor	[redacted] role=partner, [redacted]

Verification and recording posture

Rule-basis, authority, and signed-authority recording facts are rendered exactly as supplied by upstream runtime/governance metadata.

Rule-Basis Verified	true
Authority Verified	true
Signed Authority Required	true
Signed Authority Recorded	true

The original refusal was not erased. The later outcome was linked to that refusal, supervisory authority was separately recorded, and the final governed outcome changed only through the configured supervised path.

Supervision is governed recovery, not a silent bypass.

This override-path view shows that the action was not treated as an ordinary approval. The baseline refusal remained recorded, the supervised outcome was bound to the refused parent decision, and the required authority was separately verified and recorded.

Public redactions remove identities, matter identifiers, decision anchors, routing, policy, and infrastructure details while preserving evaluator-visible proof of governed exception handling.

How to Read This Supervised Override Decision Record

This Decision Record should be read as evidence of governed escalation, not legal judgment. SEAL recorded the baseline refusal, then recorded an approved supervised override after the required supervised-path conditions were satisfied. The configured downstream handoff followed that approved outcome.

A supervised override is not a bypass. It is a recorded exception with supervisory authority **before the configured downstream action proceeds**.

What to verify:

1. Baseline refusal — the original decision remained refusal.

2. Parent linkage — the later supervised outcome remained tied to that refusal.

3. Supervisory authority — required supervisory authority was separately recorded.

4. Final governed outcome — the result changed through the supervised path rather than rewriting the original refusal.

5. Downstream handoff — the configured receiver returned a successful response; external effect was not established.

6. Evidence surface — both the original refusal and later supervised outcome remain reviewable.

Decision and Downstream Handoff Alignment

This exhibit shows that SEAL is not merely producing a static artifact after the fact. A governed request reached the runtime, SEAL returned a pre-execution decision, a reviewable decision record was emitted, and the downstream handoff record reflected the same governed outcome.

The proof point is narrow: the decision record and downstream handoff record tell the same control story at the configured pre-execution path. **This exhibit does not by itself establish external institutional effect.**

Block 1 — Governed request received

A governed filing-path request entered the runtime with the declared role, workflow, stage, legal environment, and jurisdiction context needed for evaluation.

Core declared inputs
Client/runtime-supplied request context. SEAL renders these values as supplied.

Declared Role	Attorney
Declared Vertical	Administrative Law
Declared Scenario	Motion to Extend Time
Case Stage	Filing
Legal Environment / Workflow Input	Administrative Law
Requested Turnaround	Standard

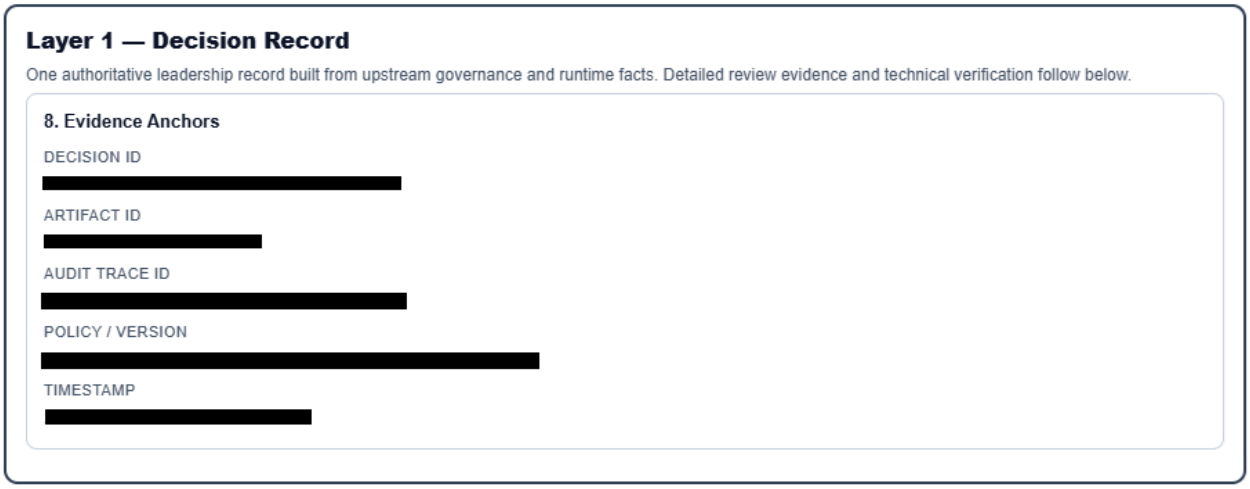
Block 2 — Decision returned

SEAL returned approval at the pre-execution control point. The governance decision, pre-execution runtime decision, final runtime decision, and decision alignment all point to the same result: approved and aligned.

Approval Code	SEAL-APP-ALLOWED-001
Enforcement Posture	Enforce (runtime decisions are applied in-line with governance policy).
Governance Decision	approval
Pre-Execution Runtime Decision	approval
Final Runtime Decision	approval
Decision Alignment	aligned

Block 3 — Artifact emitted

The runtime emitted a reviewable Layer 1 Decision Record with decision, artifact, audit-trace, policy/version, and timestamp anchor categories visible. Sensitive values are redacted.



Block 4 — Downstream handoff event

The downstream handoff record shows that, after governed approval, SEAL attempted the configured handoff and the receiving system returned a successful response.

Layer 2 — Review Evidence: Governance vs Runtime

Supplied governance, runtime, execution, and executor-gate facts for review. This record does not determine legal merits, infer execution success, infer gate status, or establish institutional effect.

Runtime Decision Path

Governance, runtime posture, pre-execution runtime, final runtime, and alignment facts supplied by upstream governance/runtime layers.

Governance Decision	approval
Pre-Execution Runtime Decision	approval
Final Runtime Decision	approval
Decision Alignment	aligned

Execution Receipt

Receipt-only execution metadata supplied to this record. The record does not call or operate downstream systems.

Status	ok
Attempted	True
OK	True
Required	True
Effective Enforcement	True
Execution Outcome	succeeded
Execution Receipt Alignment	aligned
Blocks Effective Completion	False
Control Meaning	SEAL approved this request under the firm's rules and sent it to the required firm-configured receiving system. The configured receiving system returned a successful HTTP response to SEAL's handoff request. This confirms handoff-level success only. It does not prove that the governed action was recorded, completed, docketed, accepted by an institution, or given legal or institutional effect.

Control meaning

Plain-language runtime/control meaning supplied by upstream runtime or governance metadata when present.

Plain-Language Control Meaning	SEAL approved this request under the firm's rules and sent it to the required firm-configured receiving system. The configured receiving system returned a successful HTTP response to SEAL's handoff request. This confirms handoff-level success only. It does not prove that the governed action was recorded, completed, docketed, accepted by an institution, or given legal or institutional effect.

SEAL-generated runtime artifact from a synthetic, evaluator-controlled request, shown with public redactions only. This view shows the governance decision, runtime decision, and handoff evidence are aligned: approved, enforce posture, handoff attempted, successful response. ***This confirms handoff-level success only. It does not establish recording, docketing, institutional acceptance, or legal effect.***

Could the Demo Workflow Skip SEAL?

For the scoped demo workflow, the final-submit path is governed. The **configured downstream handoff path** is available only when the workflow receives a valid governed outcome from SEAL. This exhibit does not claim production non-bypassability in every buyer environment; it shows scoped non-bypassability under the configured demo workflow.

The proof point is narrow: when the workflow is wired through SEAL, the governed request can reach the configured downstream handoff path, while direct unguided attempts are rejected.

Block 1 — Approved path through SEAL

SEAL-generated runtime artifact from a synthetic, evaluator-controlled request, shown as generated with public redactions only. This view shows the valid governed path: approved, enforce posture, downstream handoff attempted, successful response, aligned — with external institutional effect not confirmed.

Layer 1 — Decision Record

One authoritative leadership record built from upstream governance and runtime facts. Detailed review evidence and technical verification follow below.

1. Finding / Decision

FINDING
Approved

APPROVAL CODE
SEAL-APP-ALLOWED-001

2. Runtime Posture

RUNTIME MODE
Enforce

RUNTIME SUMMARY
Enforce (runtime decisions are applied in-line with governance policy).

FINAL RUNTIME DECISION
approval

DECISION ALIGNMENT
Aligned

EXECUTION / HANDOFF
Successful response to handoff request

3. SEAL Enforced?

SEAL ENFORCED?
Yes

ENFORCEMENT EFFECTIVE
Yes

4. Binding / Institutional Effect

INSTITUTIONAL / EXTERNAL EFFECT
Configured receiving system returned a successful response to SEAL's handoff request; external effect not confirmed

Governance approval, runtime approval, configured receiving-system handoff, artifact persistence, and notification delivery are not institutional effect proof. External effect is confirmed only when upstream external_commit truth and a bounded receipt establish it.

5. What Was Approved / Attempted

ACTION
Motion to Extend Time

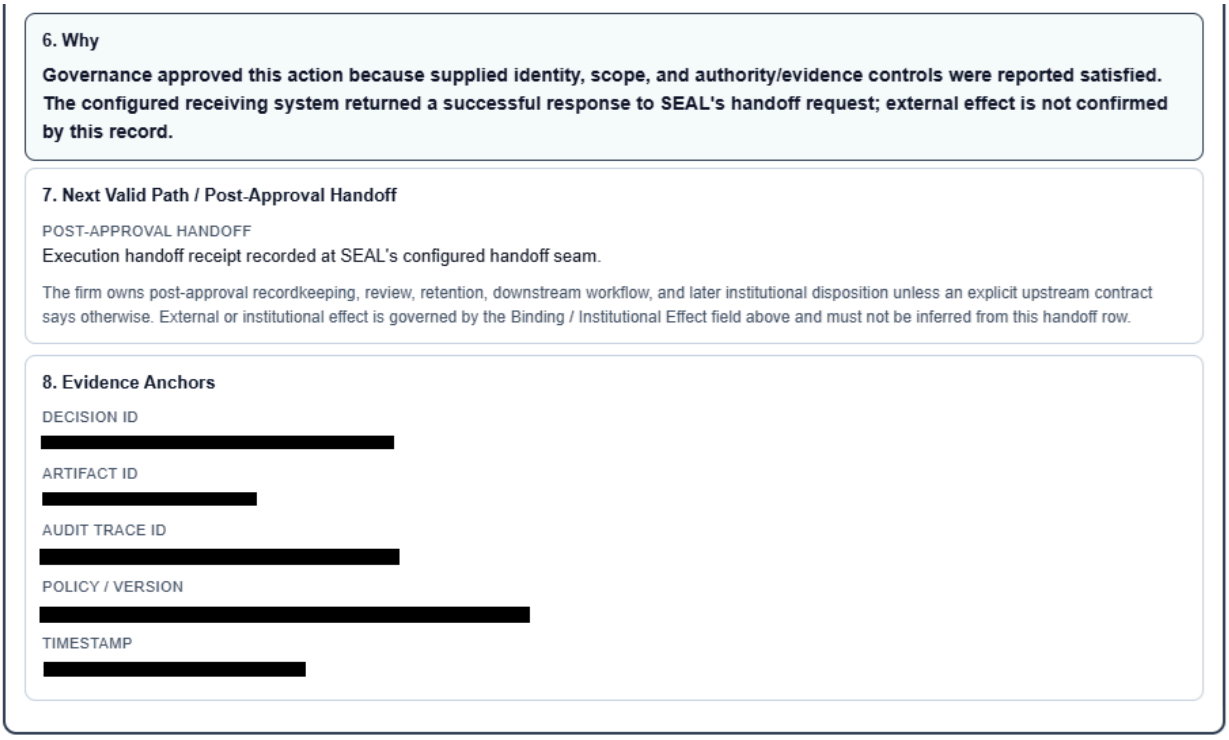
ACTOR
[redacted]

ROLE
Attorney

MATTER ID
[redacted]

DOCKET ID
[redacted]

FINAL-SUBMIT TARGET / DESTINATION
Agency Filing Portal



Approved path through SEAL

A governed filing request reached the configured downstream handoff path only after governed approval. The approval artifact and downstream handoff record share the same decision story: approval code SEAL-APP-ALLOWED-001, redacted decision / trace reference, successful handoff response, and aligned decision handling. **This exhibit does not establish external institutional effect.**

Block 2 — Direct attempt outside the governed path

A direct attempt to reach the downstream action path without a valid governed SEAL outcome was rejected by the configured demo workflow.

Check	Result
Governed SEAL outcome present	No
Downstream attempt accepted	No
Outcome	Rejected
Reason category	Invalid governed path

Block 3 — Repeat rejection under the same configured conditions

The same direct attempt was repeated and rejected again under the same configured conditions. This shows the demo workflow rejected unguided downstream attempts consistently, not as a one-off result.

Attempt	Governed outcome present	Result
Attempt 1	No	Rejected
Attempt 2	No	Rejected

Bottom takeaway

Within the configured demo workflow, access to the configured **downstream handoff path** depends on a governed SEAL outcome. Direct attempts outside the governed path are rejected.

Proof Provenance / Redactions / Evaluation Boundary

Proof Provenance & Evaluation Boundary

This packet is a public, redacted proof packet for one scoped SEAL Legal Runtime filing workflow centered on wrong-authority risk before the filing leaves the firm.

It is designed to show evaluator-visible runtime behavior, governed outcomes, decision records, downstream handoff evidence, and scoped non-bypassability evidence for that workflow. It does not expose non-public runtime internals, secrets, customer data, or production infrastructure details.

Evidence Source

The exhibits are redacted outputs from a Thinking OS™ internal / evaluator-controlled runtime environment configured to demonstrate the scoped workflow.

The packet may include:

- governed request examples
- approve, refuse, and supervised / override outcomes
- reviewable decision records
- audit trace references
- policy and rule-basis references
- integrity / review references
- execution receipt examples
- downstream handoff evidence where shown

Redactions and Evaluation Note

The public packet redacts or excludes runtime internals, secrets and credentials, tenant-sensitive identifiers, operational contact details, live internal destinations, security-sensitive configuration, non-public policy internals, and customer or prospect information.

This packet should be evaluated as proof of scoped runtime behavior, not as a representation of a completed customer production deployment. A production or enforcement deployment requires separate client-specific scoping, authority mapping, integration review, security review, and written agreement.

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.