

Legal Engineering: Verifiable Agent Controls

How to put agents on contracts, signatures, client money, and filings, and prove they stayed inside the firm's controls.



IN BRIEF

Legal engineers are being hired to put agents on real work: contracts, signatures, client money, filings. But the work a firm can safely delegate to agents is bounded by the work it can prove was done inside its own controls. This report takes five common AI-driven legal workflows and shows, for each, what a control that can be proved to a third party looks like in practice. Each workflow puts one property of provable control in the foreground. Together they cover all five.

1	The standard	A control the firm cannot prove is a control the firm does not have. Five requirements for a control on agent action, and where a control sits beside prompts and evals.	03
2	Contract review	The same edit returns the same verdict every time. Deterministic. Playbook positions digitized as controls; three agent-proposed edits, two blocked and one cleared.	06
3	Document execution	The checkpoint sits between prepared and sent. Pre-action. Field controls on an agent-prepared signature package; a check that runs after sending is a log.	08
4	Client money and communications	Verified without exposing the client file or the firm's controls. Confidential. An agent-initiated disbursement blocked against a trust balance no outside party ever sees.	10
5	Multi-tool matters	One receipt travels with the unit of work. Portable. One agent, four tools, one checkpoint, one proof that leaves every system that produced it.	13
6	Legal AI products	The buyer confirms the control fired without an account on the vendor's platform. Independently verifiable. The checkpoint embedded in a vendor's agent, and the receipt that goes to the buyer.	15
7	Court filings	The agent filing and the citation check that did not run. All five requirements at once, on an agent filing with the longest sanctions record.	17
8	The scorecard	Five workflows, five requirements, one page. What to put in the RFP and what to put in the legal engineer job description.	19

1

CHAPTER 1

The standard

A control the firm cannot prove is a control the firm does not have.

Agents now act. They open claims, draft and serve discovery, prepare documents for signature, and move client money. Adoption is close to universal: 79 percent of lawyers report using AI in practice, according to the ABA 2026 TechReport. The duty did not move with the tooling. ABA Formal Opinion 512 and Model Rule 5.3 keep supervision on the lawyer, not on the software.

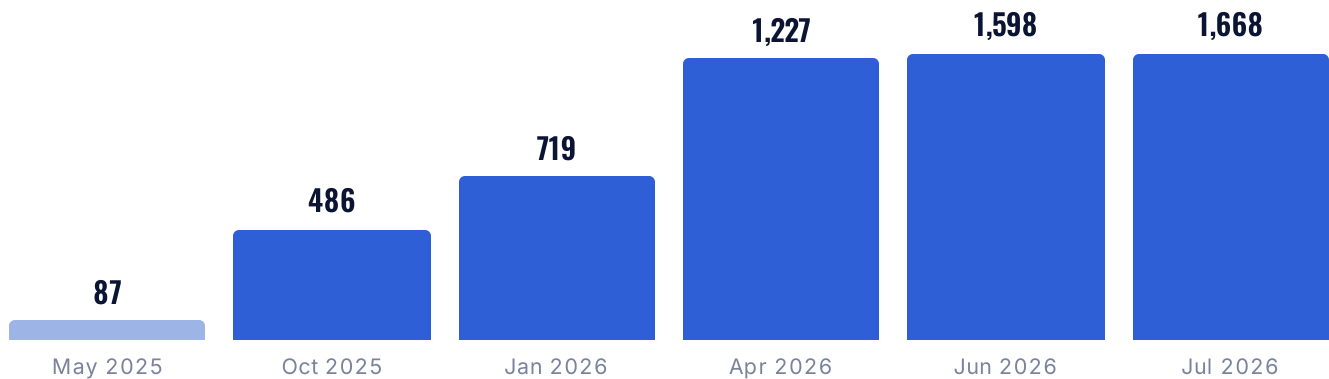
The sanctions record shows what happens when supervision is asserted rather than enforced. Most of the firms in Exhibit 1 had an AI policy. What they lacked was a way to make the policy fire on a specific action before it executed, and a way to show afterward that it had.

That is the job a legal engineer is hired to do: turn the firm's own controls into something that runs before an agent acts, and something a client, a carrier, or a court can independently verify without taking the firm's word for it. The rest of this chapter defines the standard that job is held to, locates it in the stack a legal engineer already runs, and describes the loop the work follows.

Every workflow in this report is an illustrative simulation; no live client data was used.

EXHIBIT 1

Court decisions finding reliance on AI-fabricated material grew nearly 20x in fourteen months.



Note: Cumulative court decisions worldwide in which a court found, or clearly implied, reliance on AI-hallucinated material; counts are snapshots and any figure is a floor. **Source:** Damien Charlotin, AI Hallucination Cases database; ICME Labs analysis.

EXHIBIT 2

Five requirements for a control that can be proved.

- 1 Pre-action. The check runs before the agent action.**
A control that flags a bad wire after the money moved is a log, not a safeguard. Verification has to happen while the action can still be stopped.
- 2 Deterministic. The verdict is the same every time.**
The same action, checked against the same control, must return the same answer. A check that clears an action on Monday and blocks the identical action on Tuesday proves nothing. Determinism is not a tuning target; it comes from compiling the control once into formal logic and deciding each action with a solver, not a model. The receipt in requirements 3 and 4 is only evidence because this verdict cannot vary.
- 3 Independently verifiable. Someone outside the system can confirm it.**
If only the vendor or the operator can confirm the check happened, the control is self-attested. A client, an auditor, or a regulator must be able to confirm it without trusting the operator.
- 4 Portable. The proof travels.**
Verification locked inside one platform dies there. The evidence must be checkable outside the system that produced it, by someone with no account on it.
- 5 Confidential. It works without exposing the controls or the data.**
In regulated work the control itself and the client file are often confidential. Verification that requires disclosing them is unusable where it matters most.

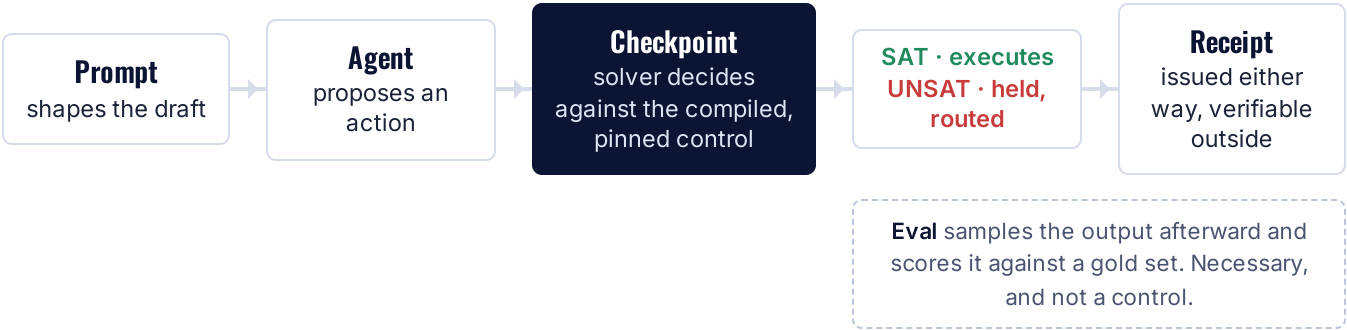
Note: The requirements restate obligations already imposed on automated action by ABA Formal Opinion 512, Model Rules 1.6, 1.15, and 5.3, FRE 902(14), GDPR Article 5(2), and EU AI Act Article 12, among others. **Source:** ICME Labs, The State of Agent Verification 2026.

THE BOUNDARY OF A PROOF

Logs assert. Receipts prove. The difference is evidence an outside party can verify.

EXHIBIT 3

Where the checkpoint sits: the control decides the action before it runs; the eval scores the output after.

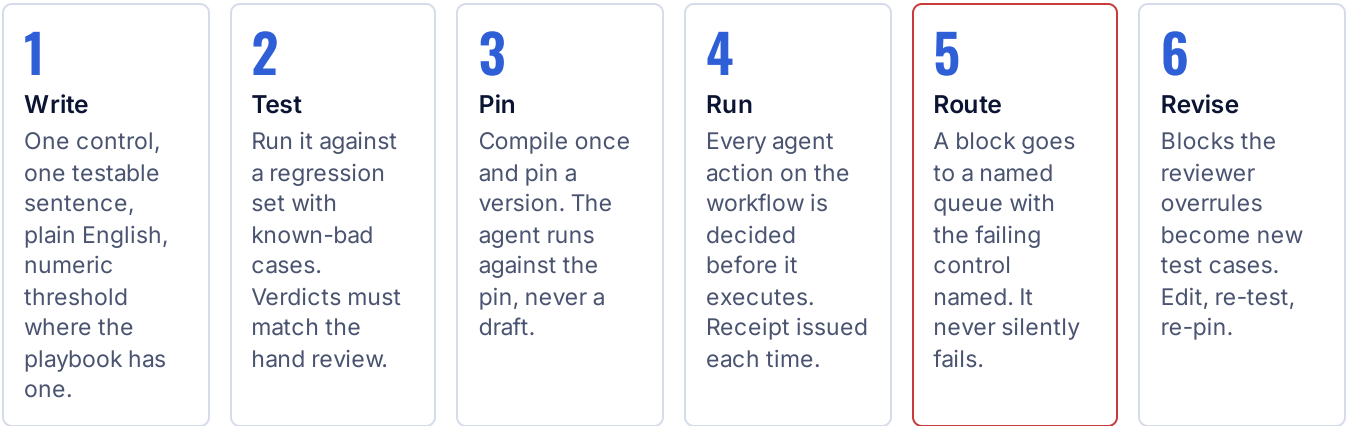


Note: Conceptual. The checkpoint decides every action on every run; the eval samples. **Source:** ICME Labs analysis.

Prompts and evals remain necessary. The control is the layer beneath them that turns a firm rule into a stop, and it is the layer a legal engineer is now expected to own. The loop below is how that ownership runs.

EXHIBIT 4

The legal engineer's loop: six steps, repeated for every control the firm runs.



← [BACK TO WRITE](#)

Note: The loop is the process-design half of the role; chapters 2 to 7 show it applied. **Source:** ICME Labs analysis.

2

CHAPTER 2 · DETERMINISTIC

Contract review

The same agent-proposed edit returns the same verdict every time.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

The playbook is the most compilation-ready control artifact a firm already owns. It has numbered positions, thresholds, and fallback positions, and most firms have already digitized it for their contract-review tool. Halden & Roe, a mid-size firm, runs a services-agreement playbook with three positions that matter here: the limitation of liability may not fall below twelve months of fees paid, governing law is Delaware, and termination for convenience requires at least sixty days of notice.

An agent reviewing a counterparty draft proposes three edits. The checkpoint tests each agent-proposed edit against the compiled playbook and returns a verdict before the redline is sent. Submit the six-month cap ten times and the verdict is UNSAT ten times. A judge-model review of the same redline can clear it on one run and flag it on the next, and a partner cannot tell which run to trust.

THE LEGAL ENGINEER'S WORK

The engineer took three positions from the digitized playbook and rewrote each as a single testable sentence with a numeric threshold where the playbook had one. Positions with a fallback ("Delaware, or New York if the counterparty insists") were split into a hard floor and a routed exception, because a fallback the agent may choose on its own is not a control.

Before the agent ran against it, the engineer built a regression set of twelve counterparty drafts, four of them known-bad, and confirmed the verdicts matched the playbook owner's hand review on all twelve. The control is pinned to version 7.1; the agent cannot run against an unpinned draft of the playbook. A block routes to the review queue with the failing position named, so the reviewing lawyer sees one position, not a whole redline.

THE CONTROL AS WRITTEN

C-4.2 The limitation of liability may not be less than twelve months of fees paid under this agreement.

C-11.1 Governing law is Delaware. Any other governing law is routed to the review queue.

C-9.3 Termination for convenience requires notice of at least sixty days.

Note: Controls are written in plain English and compiled once. The engineer never writes formal logic. **Source:** ICME Labs.

EXHIBIT 5

Three agent-proposed edits, three verdicts, decided against the same compiled playbook.

MOVE 1

Reduce liability cap to fees paid in the prior six months

UNSAT · blocked

C-4.2 sets the floor at twelve months. The edit is outside the position; the redline is held and the position is named in the review queue.

MOVE 2

Change governing law to Texas

UNSAT · blocked

C-11.1 fixes Delaware with no agent-selectable fallback. Blocked and routed for the judgment call a lawyer must make.

MOVE 3

Extend termination for convenience notice to ninety days

SAT · cleared

C-9.3 requires at least sixty days. Ninety satisfies it. The edit proceeds into the redline with no human touch.

Verification Report

RCPT-3B7E-11C4
2026-08-02 10:14:22 EDT

EDIT BLOCKED The agent's proposed edit was stopped before the redline left the firm.

On **August 2, 2026**, an agent at **Halden & Roe** proposed reducing the liability cap in the Ventor Systems MSA to **six months of fees**. Control **C-4.2** requires a floor of twelve months. The edit was **blocked** and the redline was routed to the review queue.

control	verdict	verify
msa-playbook v7.1 · C-4.2	UNSAT · 41 ms	any browser · no account

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

A fallback the agent may choose on its own is not a control.

3

CHAPTER 3 · PRE-ACTION

Document execution

The checkpoint sits between prepared and sent.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

A signature that already happened cannot be unsigned. Corbett Lane, a corporate boutique, therefore places its controls on the fields and workflow variables of the signature package, and the checkpoint runs at the moment the agent moves from "prepared" to "send." The same four checks run after the envelope went out would tell the firm what went wrong. Run before, they stop it.

Here the agent assembled a package with an effective date thirty-one days in the past and no partner approval recorded. Two of four controls fail, the agent receives the two failing fields, and nothing is sent.

THE LEGAL ENGINEER'S WORK

The engineer mapped the signature workflow first, not the controls: every field the agent populates, every variable the platform sets, and the single event at which the package leaves the firm. The controls were then written against fields, not against the document text, because fields are what the agent actually sets and what the checkpoint can decide without reading the agreement.

The authorized signatory list is an external reference the control reads at decision time, so the engineer versioned the list and pinned the control to it; a signer added to the list after the pin does not clear until the pin moves. The regression set was twenty historical packages, six of which had been caught by hand in the prior year. All six blocked. A block returns the failing field names to the agent so it can correct and resubmit; only a second failure on the same package escalates to the review queue.

THE CONTROL AS WRITTEN

C-E.1 Every signer must appear on the client's authorized signatory list, version as pinned.

C-E.2 The counterparty legal entity on the package must match the legal entity on the matter record.

C-E.3 The effective date may not precede the send date.

C-E.4 The package must carry one recorded approval from a lawyer of partner rank.

Note: Field-level controls decide on values the agent asserts, not on the agreement's meaning. **Source:** ICME Labs.

EXHIBIT 6

Four field controls on an agent-prepared package, two failures, no envelope sent.

C-E.1 Signer authority	All three signers appear on the Aldergate authorized signatory list, pin 2026-06.	pass
C-E.2 Counterparty entity	"Aldergate Holdings, Inc." matches the legal entity on matter 2026-0417.	pass
C-E.3 Effective date	Effective date 2026-07-02 precedes the send date 2026-08-02 by 31 days.	fail
C-E.4 Partner approval	No approval recorded. Control requires one approver of partner rank.	fail

Verification Report

RCPT-9A21-F0D8
2026-08-02 15:47:03 EDT

SEND BLOCKED

The agent's signature package was held before it left the firm.

On **August 2, 2026**, an agent at **Corbett Lane** attempted to send the Aldergate Holdings services agreement for signature. Two controls failed: **C-E.3, effective date preceded the send date**, and **C-E.4, no partner approval recorded**. The package was **held**. No envelope was sent.

control

execution-controls v3.4

verdict

UNSAT · 2 of 4 failed · 38 ms

verify

any browser · no account

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

Controls written against fields decide what the agent set, not what the agreement means.

4

CHAPTER 4 · CONFIDENTIAL

Client money and communications

Verified without exposing the client file or the firm's controls.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

Two duties meet in this workflow. Rule 1.15 requires the firm to safeguard client property held in trust. Rule 1.6 requires the firm to keep the client's information confidential. A control that proves the first by disclosing the second has not solved the problem. Merrow Bay Legal, a plaintiff firm, places three controls on its practice-management agent: no disbursement from trust may exceed the client's ledger balance, no client communication goes out before conflicts are cleared and an engagement letter is on file, and no communication goes to a party the firm knows to be represented.

The agent attempts a settlement disbursement of \$42,500 against a ledger balance of \$38,200. The disbursement is blocked. A malpractice carrier, a bar auditor, or the client can later confirm the control fired without being shown the balance, the client's name, the matter, or the control text.

THE LEGAL ENGINEER'S WORK

The engineer's first decision was which values the control reads and where they come from. The ledger balance is read from the trust accounting system at decision time, not from the agent's context, so an agent that has been told the wrong balance cannot clear itself. The represented-party list is read the same way. Each source is named in the control and pinned.

The second decision was what the receipt carries. The engineer configured the receipt to disclose the control identifier, version, timestamp, and verdict, and nothing about amounts, parties, or control text. This is the setting a bar auditor will ask about, so the engineer documented it alongside the trust reconciliation procedure. The regression set was every disbursement in the prior quarter, replayed. Two would have blocked; both had been caught by the bookkeeper. A block on a disbursement routes to the responsible lawyer and the bookkeeper together, never to the agent for retry.

THE CONTROL AS WRITTEN

C-T.1 A disbursement from trust may not exceed the client's ledger balance as read from the trust accounting system at decision time.

C-T.2 No communication to a client may be sent unless the conflicts check is cleared and an engagement letter is on file for the matter.

C-T.3 No communication may be sent to a party on the represented-party list.

Note: Values read from systems of record at decision time cannot be supplied by the agent. **Source:** ICME Labs.

EXHIBIT 7

What an outside verifier sees of an agent-initiated disbursement, and what stays inside the firm.

OUTSIDE VERIFIER SEES

- That trust control C-T.1, version 5.2, fired on an action at 2026-08-03 09:21:40 EDT
- That the verdict was UNSAT and the action was blocked before execution
- That the receipt is unaltered since issuance
- That verification required no account on the firm's system and no contact with the firm

STAYS INSIDE THE FIRM

- The client's identity and matter
- The ledger balance (\$38,200) and the requested amount (\$42,500)
- The plain-English text of the control and the compiled logic behind it
- The agent's reasoning and the settlement terms

Verification Report

RCPT-52C0-A7E3
2026-08-03 09:21:40 EDT

DISBURSEMENT BLOCKED The agent's transfer from trust was stopped before it executed.

On August 3, 2026, an agent at Merrow Bay Legal attempted a disbursement from the client trust account. Control C-T.1 does not permit a disbursement exceeding the client's ledger balance. The action was blocked. No funds moved.

control	verdict	verify
trust-controls v5.2 · C-T.1	UNSAT · 44 ms	any browser · no account · no file

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

Verification that required the file would not happen. Verification that requires nothing does.

What a block does is a design decision, and it differs by workflow.

A control that stops an action has to send it somewhere. The three firm-side workflows route a block three different ways, and the legal engineer chose each one on the same three questions: can the agent fix it alone, who must see it, and how many retries before a human is required.

EXHIBIT 8

Three workflows, three routes for an UNSAT verdict.

WORKFLOW	WHAT THE AGENT RECEIVES	WHERE THE BLOCK GOES	RETRIES BEFORE A HUMAN
Contract review	The failing position identifier and its threshold	REVIEW QUEUE with one position named, not the whole redline	None. A position outside the playbook is a lawyer's call by definition.
Document execution	The failing field names and the required values	BACK TO THE AGENT to correct and resubmit; REVIEW QUEUE on a second failure	One. Field errors are usually the agent's to fix.
Client money	A block notice only; no amounts, no retry path	RESPONSIBLE LAWYER AND BOOKKEEPER together, with the ledger	None. The agent is never allowed to retry a trust disbursement.

Note: Routing is configured per control, not per workflow; the table shows the default for each. Source: ICME Labs analysis.

A block that goes nowhere is a log with a red label.

5

CHAPTER 5 · PORTABLE

Multi-tool matters

One receipt travels with the unit of work.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

Real matters do not live in one tool. Ashgrove Litigation, a defense firm, gives its agent access to four: a research database, a drafting environment, the docketing calendar, and the court filing system. The agent's unit of work is one motion, and it touches all four through tool calls. If each tool keeps its own verification record, the partner has four records in four formats in four systems, and the client has none.

The fan-in pattern routes every tool call through a single checkpoint before it executes. The receipt is issued for the unit of work, not per call, and it leaves every system that produced it. The carrier, the client, and the auditor receive the same artifact and verify it the same way, with no login to any of the four tools.

THE LEGAL ENGINEER'S WORK

The engineer's job here was topology, not control text. Each tool exposes its own hooks and its own idea of a policy; the engineer declined all four and put one checkpoint at the orchestration layer, where every tool call passes as a structured action before dispatch. The controls are written once against the action schema (tool, operation, arguments), so a new tool added next quarter inherits them without a rewrite.

The engineer defined the unit of work as the motion, keyed to the matter number, so the receipt chain has one root per motion rather than one per call. Controls include a calendar rule (no filing action may be dispatched unless the docket deadline for that motion is at least one business day out) and a scope rule (the filing tool may only be called with a document that passed the drafting-environment checkpoint). Testing replayed one prior month of tool calls against the checkpoint before the agent was allowed to dispatch a live call.

THE CONTROL AS WRITTEN

C-M.1 Every tool call on a matter is decided by the matter checkpoint before dispatch, whichever tool it targets.

C-M.2 A filing action may not be dispatched unless the docket deadline for the motion is at least one business day after the dispatch time.

C-M.3 The filing tool may only be called with a document identifier that carries a cleared verdict from the drafting checkpoint.

Note: Controls written against the action schema apply to tools added later without rewriting. **Source:** ICME Labs.

EXHIBIT 9

One agent's calls to four tools fan in to one checkpoint; one receipt fans out to everyone who needs it.



Note: Tool categories are generic; no vendor product is depicted. Source: ICME Labs analysis.

Verification Report

RCPT-D41F-8B20
2026-08-04 11:08:51 EDT

UNIT OF WORK CLEARED

Fourteen tool calls on one motion; every call decided before dispatch.

Between **August 3 and 4, 2026**, an agent at **Ashgrove Litigation** made **fourteen tool calls** across four tools to prepare and file a motion on matter 26-1183. Each call was decided by the matter checkpoint before dispatch. **Fourteen cleared, none blocked**. The receipt covers the motion as one unit of work.

control

matter-controls v2.0 · C-M.1 to C-M.3

verdict

SAT · 14 of 14

verify

any browser · no account on any tool

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

The work you can prove is the work you can delegate.

6

CHAPTER 6 · INDEPENDENTLY VERIFIABLE

Legal AI products

The buyer confirms the control fired without an account on the vendor's platform.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

The legal engineer at a vendor has a different reader in mind: the general counsel or risk officer at the enterprise buying the product. Northline, a contract-drafting platform, sells into insurers. Pemberton Mutual's general counsel will approve production use on one condition: that the platform's agent follows Pemberton's own drafting controls, and that Pemberton can confirm this without depending on Northline's word.

A dashboard inside Northline's product that reports "controls enforced" is Northline's account of itself, and a risk officer is right to discount it. The receipt is different in kind. Pemberton's general counsel verifies it in a browser, with no Northline login, and would get the same answer if Northline ceased to exist. The vendor's enforcement claim becomes the buyer's evidence.

THE LEGAL ENGINEER'S WORK

Northline's legal engineer owns two things the firm-side engineer does not: a multi-tenant control library and a customer-facing receipt. Each customer's controls are that customer's; Northline staff can run them but not read them, and the compiled form is what the checkpoint holds. The engineer built a control-authoring flow so Pemberton's own legal ops team writes and versions Pemberton's controls inside Northline, and Northline's product agent is pinned to whichever version Pemberton has approved.

The receipt is issued to Pemberton, not to Northline. The engineer wrote the verification page that Pemberton's risk team bookmarks, the one that takes a receipt identifier and returns a verdict with no Northline credentials. Sales now sends that page in the security questionnaire response instead of a SOC 2 excerpt. The engineer's regression set is each customer's own historical drafts, run under that customer's controls, with results shared back to the customer as receipts rather than as an accuracy percentage.

THE CONTROL AS WRITTEN (CUSTOMER-AUTHORED)

PM-D.1 No indemnity clause may be drafted with an uncapped obligation on Pemberton.

PM-D.2 Every drafted clause referencing coverage limits must cite the policy form identifier in the matter record.

PM-D.3 Drafts for a regulated line of business must carry the state filing reference before the draft leaves the platform.

Note: Controls are authored and versioned by the buyer; the vendor's agent is pinned to the buyer-approved version. **Source:** ICME Labs.

EXHIBIT 10

Two ways a vendor can answer "how do we audit this" about its agent's actions.

	VENDOR DASHBOARD	VERIFICATION RECEIPT
Who authored it	The vendor, about its own behavior	The checkpoint, at the moment of decision
When it exists	After the action, as a summary	Before the action runs; a failed check stops it
Who can check it	Anyone with a vendor account, trusting the vendor	Anyone with the receipt, trusting no one
What it exposes	The buyer's controls and matters, to the vendor's staff	That the control fired; nothing about the controls or the matter
What happens if the vendor is gone	The evidence is gone	The receipt still verifies

Note: Illustrative simulation; no specific product is assessed. Source: ICME Labs analysis.

Verification Report

RCPT-6E90-C2B7
2026-08-05 16:02:19 EDT

DRAFT BLOCKED

The vendor agent's draft was stopped before it reached the buyer.

On **August 5, 2026**, the Northline drafting agent, running under **Pemberton Mutual's** controls, attempted to release a draft containing an **uncapped indemnity obligation**. Control **PM-D.1** **does not permit an uncapped obligation on Pemberton**. The draft was **blocked**. Receipt issued to Pemberton Mutual.

control
pemberton-drafting v1.3 · PM-D.1

verdict
UNSAT · 39 ms

verify
any browser · no vendor account

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

7

CHAPTER 7 · ALL FIVE REQUIREMENTS

Court filings

The agent filing and the citation check that did not run.

● 1 PRE-ACTION

● 2 DETERMINISTIC

● 3 INDEPENDENT

● 4 PORTABLE

● 5 CONFIDENTIAL

The filing workflow has the longest public record of failure, and the record points in one direction. The 1,668 decisions in the Charlotin database do not describe firms whose citation-checking tools were weak. They describe filings on which the citation check never ran. Courts have repeatedly described the duty to verify citations as non-delegable, and sanctions have escalated from the \$5,000 in *Mata v. Avianca* in 2023 to six-figure combined awards in 2026.

Meridian Law has one control on filings: a citation verification must have run and passed on the document before the agent may submit it. The agent attempts to file a brief in the Southern District of New York. The verification has not run. The filing is blocked.

This is the workflow where all five requirements do visible work at once. The check runs before submission. It returns the same verdict for the same document every time. Opposing counsel or the court can confirm the control fired without contacting the firm. The receipt leaves the filing system and the document platform. And the court sees that the check ran, not the brief's drafting history or the control text.

THE LEGAL ENGINEER'S WORK

The control looks trivial and the engineering is in the predicate. "A citation verification has run and passed" has to mean something the checkpoint can decide: a verification record, from a named tool, on this document identifier at this content hash, with a pass result and a timestamp after the last edit. The engineer wrote the control to that predicate so that an agent cannot satisfy it by running the checker on an earlier draft and editing afterward.

The engineer also decided what a block does. It does not retry. It routes to the filing lawyer with the document, the missing verification, and the docket deadline on one screen. The regression set was the firm's last hundred filings; three would have blocked, all three because the checker ran before a final edit. Enforcement first, then proof, then scope.

THE CONTROL AS WRITTEN

C-F.1 No filing may be submitted unless a citation verification from the firm's designated checker has passed on the document at its current content hash, with a timestamp after the document's last edit.

Anatomy of a receipt: what it carries, what it proves, and what it leaves out.

Verification Report

RCPT-7F3A-2E91
2026-08-04 14:52:07 EDT

FILING
BLOCKED

The agent's filing was stopped before it was submitted.

On **August 4, 2026**, an agent at **Meridian Law** attempted to file a brief with the U.S. District Court, S.D.N.Y. Control C-F.1 requires a passed citation verification at the document's current content hash. None was on record. The filing was **blocked**, and nothing was submitted.

control	verdict
filing-controls v3.2 · C-F.1	UNSAT · 36 ms

verify
any browser · no account

- 1

Receipt identifier. The handle an outside party pastes into a verification page. Tamper-evident: any change to the underlying record is detectable.
- 2

Decision timestamp. When the verdict was rendered, which is before the action, not when the action was logged.
- 3

Plain-language report. What a lawyer reads in ten seconds. Rendered from the proof, not authored separately.
- 4

Control identifier and version pin. Names the control and the exact version it was decided against. Because the verdict is a solver's, not a model's, the receipt attests to a decision anyone can reproduce; a receipt over a probabilistic verdict would prove only that a model guessed.
- 5

Verification path. No account on the firm's systems, no contact with the firm, no access to the file.
- 6

Not present. The brief, the citations, the drafting history, the control text, the agent's reasoning. The receipt proves the control fired against the facts the agent asserted, not that those facts are true of the world.

Note: Illustrative simulation. Source: ICME Labs verification report rendering.

The report is what you read. The receipt is what you cannot fake.

A receipt removes one question from the sanctions record: whether the check ran at all. It does not make the brief correct, and it does not replace the lawyer who reads it. It gives that lawyer, and the court, and the carrier, the same artifact to check. Firms that can prove their filing controls held can put agents on filings.

8

CHAPTER 8

The scorecard

Five workflows, five requirements, one page.

EXHIBIT 12

The same workflows as most firms run them today.

WORKFLOW, AS COMMONLY RUN	1 PRE-ACTION	2 DETERMINISTIC	3 INDEPENDENT	4 PORTABLE	5 CONFIDENTIAL
Contract review judge-model redline review	●	●	●	●	●
	Can hold the redline	Probabilistic	Vendor report	In the tool	Judge sees the draft
Document execution platform audit log	●	●	●	●	●
	After send	Record stable	Self-attested	Exportable	Log shows fields
Client money monthly reconciliation	●	●	●	●	●
	After transfer	Ledger math	Auditor sees file	Paper travels	Requires the file
Multi-tool matters per-tool logs	●	●	●	●	●
	After the fact	Records stable	Four self-reports	Dies in each tool	Varies by tool
Legal AI products vendor dashboard	●	●	●	●	●
	Summary after	Depends on vendor	Trust the vendor	Vendor account	Vendor sees all
Court filings lawyer spot check	●	●	●	●	●
	If it happens	Varies by day	No record	None	Nothing exposed

● Meets the requirement ● Partially or conditionally ● Does not meet it

Note: Characterizations reflect the most common control in use for each workflow; implementations vary. Source: ICME Labs analysis.

EXHIBIT 13

The same workflows with a verifiable control. Shaded cell: the requirement each chapter teaches.

WORKFLOW	1 PRE-ACTION	2 DETERMINISTIC	3 INDEPENDENT	4 PORTABLE	5 CONFIDENTIAL
Contract review	●	●	●	●	●
Document execution	●	●	●	●	●
Client money	●	●	●	●	●
Multi-tool matters	●	●	●	●	●
Legal AI products	●	●	●	●	●
Court filings	●	●	●	●	●

Note: Grade any live implementation, including ours, against the five requirements directly. Source: ICME Labs analysis.

Put the five requirements in the RFP and the loop in the job description.

Five questions for the RFP

Ask any vendor of agent controls, including ICME Labs, to state the following in writing.

1. Where the check runs, before the action or after it.
2. Whether the verdict is repeatable for the same action and control.
3. Who outside the vendor's system can independently verify that the check ran, and how.
4. Whether the proof leaves the vendor's platform, and in what form.
5. Whether verifying it requires disclosing the firm's controls or data.

Three lines for the legal engineer job description

The postings describe prompt design and workflow mapping. Few describe proof. Three additions.

- Translate firm playbooks and policies into plain-English controls that are enforced before an agent action executes; own the control library, its regression sets, and its version pins.
- Define, for each agent workflow, the unit of work, the escalation path on a block, and the receipt a client, carrier, or auditor can verify without access to our systems.
- Reserve human review for the judgment only a human may render; automate the checks a human was never going to perform reliably at volume.

About the author. Houman Shadab is co-founder of ICME Labs and a Fellow at Stanford CodeX. He is an award-winning legal scholar, three-time Congressional witness, and spoke by invitation at the Federal Reserve Bank of New York's 2026 Innovation Conference on turning law into verified code. Contact: houman@icme.io.

About ICME Labs. ICME builds Preflight, pre-action verification for AI agents: plain-English controls, deterministic enforcement, and tamper-evident cryptographic receipts anyone can verify. Every workflow in this report was rendered with it. Translation methodology adopted from AWS Automated Reasoning Checks (arXiv:2511.09008), cryptographic verification layer added by ICME (arXiv:2602.17452). icme.io