

AI-Assisted Chain-of-Title: Verifying Pre-IPO Secondaries with LLMs

An evidence-linked architecture for share provenance, stacked SPVs, transfer restrictions and controlled settlement

Prepared by Matchpoint Partners

Author attribution pending CK approval

August 2026

ABSTRACT

Background. Pre-IPO secondary buyers and intermediaries must connect private-company records, transaction instruments, stacked SPVs, beneficial ownership, transfer restrictions, sanctions and settlement controls before capital moves. **Objective.** This paper develops an AI-assisted chain-of-title operating model for A8 family-office and UHNW buyers and A9 brokers, investment banks and platforms. **Approach.** The analysis reviews 32 primary and authoritative sources available through 1 August 2026 and joins immutable documents, structured claims, entity resolution, a knowledge graph, deterministic rules, Claude-assisted cited analysis and named human approvals. **Findings.** LLMs can support extraction, comparison and exception explanation within a controlled architecture. Corporate-record, legal, compliance, investment, finance and settlement authorities retain consequential determinations. **Implications.** Every material proposition should keep its source, period, authority, permission, reviewer and unresolved-condition status. The worked scenario, weights, thresholds and roadmap are unverified illustrative management assumptions; attributed Matchpoint or client revenue, cash cost reduction, loss reduction and alpha remain USD 0 until approved observed evidence exists.

Highlights

Primary users. A8 pre-IPO secondary buyers and A9 pre-IPO secondary intermediaries.

Evidence unit. An atomic claim with exact source location, authority, period, permission, conflict state and reviewer.

Architecture. Immutable sources feed extraction, entity resolution, a provenance graph, rules, cited Claude analysis and controlled workflow.

Decision boundary. The system prepares evidence and exceptions; named specialists and transaction authorities make consequential decisions.

Economics. Attributed revenue, cash saving, loss reduction and alpha remain USD 0 until observed evidence is approved.

JEL Classification: C88, D83, G23, G24, K22, K23, K24, L86, O33

Keywords: pre-IPO secondaries, chain of title, Claude, large language models, knowledge graphs, entity resolution, special-purpose vehicles, beneficial ownership, transfer restrictions, sanctions, settlement

Research paper only. This document is not investment, legal, regulatory, compliance, accounting, audit, tax, privacy, cybersecurity or technology advice. Its worked scenario, score weights, thresholds, times and economics are unverified illustrative management assumptions.

1. INTRODUCTION

Pre-IPO secondary transactions sit at the intersection of private-company law, contract, securities regulation, corporate records, beneficial ownership and operational settlement. A buyer may receive an attractive commercial narrative and a large data room while still lacking a complete answer to the basic question: what precise interest is being sold, through which legal chain, subject to which restrictions, by which authorised person, and with whose consent? The difficulty increases when exposure is held through nominees, custodians, aggregators, special-purpose vehicles or several stacked entities. Each layer can introduce a different register, governing document, transfer instrument, approval process, economic entitlement and disclosure boundary.

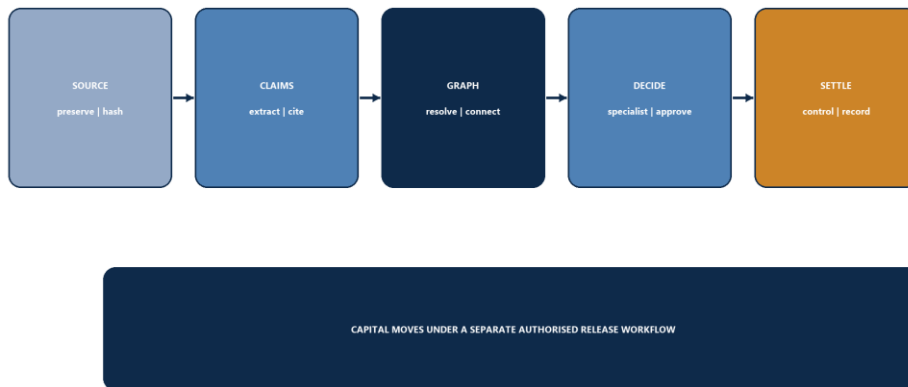
This paper develops an AI-assisted chain-of-title operating model for A8 pre-IPO secondary buyers, including family offices and ultra-high-net-worth investors, and A9 intermediaries, including brokers, investment banks and platforms. Its purpose is to help those parties organise evidence, expose gaps and route decisions before capital moves. The model uses document extraction, entity resolution, a knowledge graph, deterministic rules, sanctions and beneficial-ownership checks, cited large-language-model analysis and named human approvals. It does not delegate legal title, securities-law, transfer-restriction, sanctions, suitability, tax or investment decisions to an LLM.

The phrase **chain of title** is used here as an operational diligence shorthand. For a direct share, the relevant evidence can include the issuer's share ledger or register of members, the certificate or electronic record, subscription and prior-transfer instruments, restrictions, consents, authority and settlement instructions. For an SPV interest, the chain may also include the SPV's formation and good-standing evidence, constitutional documents, member or partnership register, capital accounts, nominee or custody arrangements, upstream ownership, downstream issuer exposure, economic waterfalls, pledges, liens and prior transfers. Applicable law and transaction structure determine the legal significance of each item. Delaware law, for example, recognises transfer restrictions subject to statutory conditions; US federal securities law separately requires an available registration exemption for a resale of restricted securities [1-5].

The analytical unit in this paper is an **evidence-backed claim**, not a document summary. A claim states one proposition, points to the exact source and location, records the source date and authority, identifies the person or system that supplied it, carries a confidence and conflict status, and routes to an accountable reviewer. This structure follows the central insight of the Beneficial Ownership Data Standard: data statements are claims with their own provenance, dates and sources, and apparently inconsistent statements can coexist until they are resolved [14-15]. W3C PROV-O provides a compatible vocabulary for entities, activities, agents and derivation [28].

The operating answer developed through the paper is summarised below.

Research question	Operating answer
What should AI extract?	Parties, entities, instruments, security classes, quantities, dates, signatures, approvals, restrictions, rights, ownership statements and source locations.
What belongs in the graph?	Evidence-backed claims and typed relationships among issuers, securities, holders, beneficial owners, SPVs, agents, instruments, approvals and transfer events.
What can an LLM decide?	It can classify, compare, explain and propose a cited exception analysis within an approved schema; it cannot deliver legal clearance or confirm title.
How are transfer restrictions tested?	Deterministic rules identify applicable clauses, notice requirements, rights of first refusal, consent conditions and unresolved facts; qualified counsel and authorised issuer parties determine their effect.
How is counterparty risk scored?	A transparent triage rubric combines identity, authority, provenance, sanctions, adverse evidence, payment and settlement exceptions; reviewers retain the approval decision.
What allows capital to move?	A release pack containing resolved evidence, named approvals, permitted payment instructions, settlement controls and an explicit record of residual conditions.

Source-to-settlement evidence chain**Figure 1. Source-to-settlement evidence chain**

Source: Matchpoint chain-of-title control framework; legal and evidence context [1-17,28].

The contribution is practical. Sections 2 to 6 define the decision perimeter, legal and evidential objects, source hierarchy and graph. Sections 7 to 12 specify the extraction, entity-resolution, restriction, counterparty, Claude and citation architecture. Sections 13 to 17 turn the design into a controlled workflow, worked example, scorecard, evaluation programme and security model. Sections 18 to 20 provide an implementation roadmap, release checklist, claims register and limitations.

2. A8 AND A9 DECISION PERIMETER

2.1 A8 pre-IPO secondary buyers

A8 buyers need an evidence base that joins commercial underwriting to executable ownership. Their questions normally span five layers: the issuer and security; the seller and its authority; the legal route by which the seller acquired or controls the interest; restrictions and approvals that govern the proposed transfer; and the mechanism by which cash and the acquired interest will exchange. A family office may use an adviser, custodian, nominee or SPV, yet remains responsible for its own investment, legal, tax, compliance and governance decisions.

The buyer's investment committee can use an AI-assisted dossier to examine provenance, concentration, pricing basis, information rights, governance exposure and residual conditions. It should receive a clear separation between observed documents, third-party statements, analyst conclusions, counsel determinations and unresolved assumptions. The system should never convert a seller representation into an observed fact merely because it appears in signed documentation.

2.2 A9 intermediaries

A9 intermediaries may source, introduce, structure, syndicate, arrange or facilitate a transaction. Their exact regulated role, duties and permitted activities depend on jurisdiction and engagement. The operating model therefore records role and authority at the transaction level. It does not assume that a broker, platform, placement agent or investment bank has verified ownership, holds client money, provides legal advice or controls issuer settlement.

An intermediary can use the system to standardise intake, identify documentary gaps, avoid presenting incompatible statements to counterparties, control disclosure permissions and maintain a defensible hand-off. The intermediary's release package should state what it has received, what it has tested, what remains third-party or management supplied, which specialists made determinations, and which conditions remain before closing.

2.3 Decision rights

Decision	AI-assisted contribution	Required authority
identify parties and entities	extract and resolve names, identifiers and addresses	KYC or compliance owner confirms identity population
reconstruct ownership events	connect claims, instruments and dates	transaction lead and qualified counsel review the evidential chain
interpret a transfer restriction	locate clauses and compare facts to a rule schema	qualified counsel determines legal effect
confirm issuer records	reconcile supplied extracts and responses	issuer or authorised transfer agent controls the authoritative record
screen sanctions	prepare name, identifier and ownership matches	compliance owner resolves matches and applicable rules
assess counterparty risk	calculate transparent triage score and exceptions	authorised risk or transaction committee approves
approve investment	present evidence and residual conditions	buyer's authorised investment committee
release transaction information	enforce permission and redaction rules	information owner and transaction authority
release payment	compare approved instructions and closing conditions	authorised finance, escrow, custodian or settlement control

A8 buyer and A9 intermediary decision rights



Figure 2. A8 buyer and A9 intermediary decision-rights map

Source: Matchpoint ICP and decision-rights framework.

2.4 The three-state control language

Every material diligence proposition should resolve to one of three states. **Supported** means an approved source supports the proposition within its stated scope and date. **Conditioned** means the proposition depends on a named consent, event, document or specialist determination. **Unresolved** means the evidence is absent, conflicted, stale, illegible or outside the reviewer's authority. This language creates a useful barrier against false certainty. It also allows an investment committee to distinguish a curable closing condition from an unbounded provenance gap.

3. WHAT CHAIN OF TITLE MEANS FOR PRIVATE SECURITIES

3.1 Direct registered shares

For direct registered shares, the chain begins with the issuer and the exact security class. The diligence file should identify the issuer's legal name and jurisdiction, the class and rights of the security, the registered holder, quantity, certificate or electronic position, acquisition event, consideration, relevant legends, encumbrances and proposed transfer. Delaware General Corporation Law section 159 recognises shares as personal property transferable as provided by Article 8 of the Uniform Commercial Code [3]. Section 202 addresses restrictions on transfer and when they may be enforceable against holders and transferees [2]. These provisions make the actual instrument, notice and knowledge facts important; a generic statement that shares are transferable is inadequate.

Federal securities law creates a separate resale question. SEC guidance explains that private-market securities may remain restricted and that resales require registration or an available exemption [1]. Rule 144 offers a non-exclusive safe harbour subject to its conditions; Section 4(a)(7) provides another statutory route with conditions that include purchaser status, absence of general solicitation and specified information [4-5]. An operational chain therefore needs both a corporate-record path and a securities-law path. Satisfaction of one does not establish satisfaction of the other.

Transfer agents perform a critical recordkeeping function in securities markets, including recording ownership changes, maintaining records and cancelling or issuing certificates [6]. Many private companies manage records directly or through private-market service providers. The system must identify who actually controls the relevant ledger and what evidence that party requires. A screenshot, cap-table export or seller-provided certificate can inform diligence while remaining subordinate to the authorised record and closing mechanics.

3.2 SPV and fund interests

An SPV transaction may transfer an interest in an entity whose asset is the issuer security. The investor can therefore acquire exposure without becoming a direct shareholder. The evidential path then has at least two linked chains: ownership and transferability of the SPV interest, and ownership and economic rights of the SPV in the underlying issuer security. Each chain needs its own governing law, register, instruments, restrictions, approvals and encumbrance analysis.

Stacked SPVs add another chain for every layer. A buyer of an interest in SPV C may depend on SPV C's interest in SPV B, SPV B's interest in SPV A, and SPV A's registered or beneficial interest in the issuer. Economic rights can diverge from voting, information, distribution and transfer rights at each level. Fees, carried interest, reserves and allocation mechanics can change the exposure. The graph should model the underlying security separately from the contractual economic entitlement.

3.3 Nominees, custodians and beneficial owners

Legal ownership, registered holding, custody, nominee capacity, control and beneficial ownership are different relationships. OpenOwnership guidance expressly models nominee relationships rather than collapsing nominees into beneficial owners [15]. FATF's beneficial-ownership guidance supports a multi-pronged approach using adequate, accurate and up-to-date information [10]. UAE requirements similarly call for identification and verification of beneficial owners through reliable independent sources [11-13].

The system should store each relationship with its own type, effective period, source and reviewer. A person can be the ultimate beneficial owner of an SPV while a corporate services provider is its registered office, a nominee is its registered shareholder, an investment manager has contractual authority, and a custodian controls settlement. Entity resolution should connect these identities without treating them as interchangeable.

3.4 Transfer events

A chain is temporal. Each issuance, subscription, assignment, sale, contribution, conversion, split, cancellation, pledge, release, nominee declaration or merger can alter the position. The graph must represent the before and after quantity, the instrument, its effective date, the parties, the approvals and the ledger evidence. Backdated, undated or conditionally effective instruments should retain those states. An LLM may extract a date printed on a document; the workflow must separately establish execution, delivery, effectiveness and recordation where these distinctions matter.

Object	Minimum fields
issuer	legal name, jurisdiction, registration identifier, status, authoritative source
security	class, rights, par or nominal value where applicable, certificate or position identifier, legend
holder	legal identity, capacity, address, identifier, effective period
beneficial owner	person or entity, ownership or control basis, percentage or range, evidence, verification date

Object	Minimum fields
instrument	type, parties, execution date, effective date, signature state, governing law, source hash
transfer event	from, to, quantity, security, consideration, event date, conditions, recordation evidence
restriction	clause, affected security or interest, trigger, process, waiver or consent evidence
encumbrance	secured party, affected asset, scope, filing or instrument, status, release evidence
approval	authority, decision, date, scope, conditions, source

4. STACKED SPVS AND PROVENANCE

4.1 A graph rather than a folder tree

Folder structures organise files; they do not express the legal and economic relationships among them. A document can cover several entities, securities and events. One entity may appear under historical names or abbreviations. Two signed instruments can conflict. A graph lets the analyst ask which claims support a relationship, what changed during a period, which upstream beneficial owners cross a threshold, and which proposed transfer depends on an unresolved approval.

The recommended graph separates **real-world objects** from **evidence claims**. An entity node represents the system's current resolved identity. A claim node records that a specific source asserted a particular relationship or attribute. Reviewers may promote a claim to accepted operating status, reject it, or leave it unresolved. The original claim remains immutable for provenance. This matches BODS 0.4's claim-based design and avoids silently rewriting history [14].

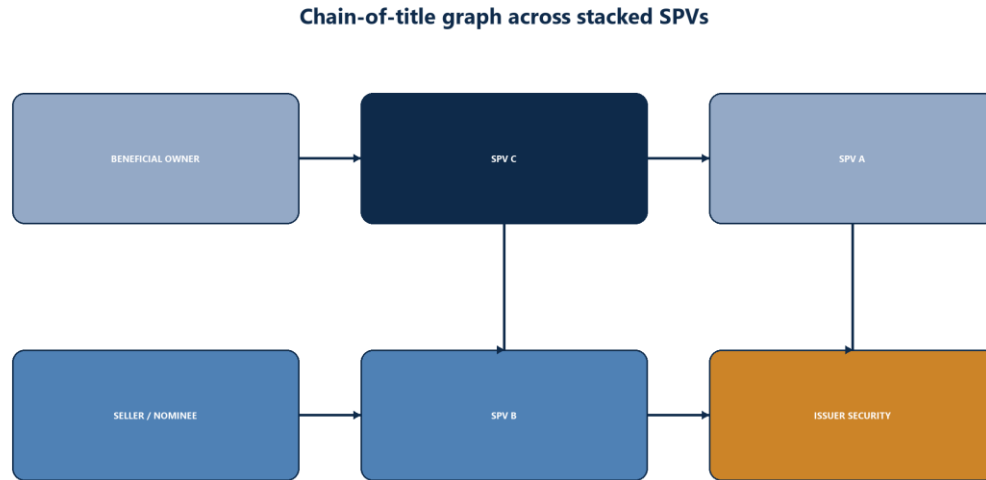


Figure 3. Chain-of-title knowledge graph across stacked SPVs

Source: Matchpoint graph model; beneficial-ownership and provenance context [10-17,28,32].

4.2 Bi-temporal records

Two time dimensions are useful. **Valid time** records when a relationship or fact is said to apply in the real world. **System time** records when the claim entered or changed status in the diligence system. A register extract dated 15 July may state ownership effective from 1 June but arrive on 20 July. The three dates should remain distinguishable. This makes late evidence, backdated instruments and post-closing updates visible.

Each claim should also carry an “observed”, “represented”, “derived” or “determined” evidence class. Observed evidence comes directly from an authoritative system or original document accessible to the reviewer. Represented evidence is supplied by a party. Derived evidence is calculated or connected from other claims. Determined evidence records a specialist or authorised decision. The labels describe provenance; they do not make the underlying proposition true.

4.3 Identity keys

Entity resolution should begin with durable identifiers and jurisdictional context. Relevant identifiers may include company registration numbers, legal-entity identifiers, tax identifiers where lawfully processed, passport or national identifiers within a restricted KYC service, addresses, dates of birth, incorporation dates and account identifiers. GLEIF separates Level 1 entity reference data, described as who is who, from Level 2 relationship data, described as who owns whom [16-17]. Its accounting-consolidation relationships do not replace beneficial-ownership or transaction-specific analysis, yet the model offers a valuable separation between identity and relationship claims.

Name similarity is a candidate generator. It is not a confirmation method. The system should assign matches from exact identifiers, corroborated attributes and reviewer decisions, and should preserve aliases and historical names. A sanctions-screening service should receive the identifiers and ownership relationships it needs under applicable law and approved privacy controls.

4.4 Graph invariants

Deterministic graph tests expose structural errors before narrative review. Examples include a transfer quantity greater than the seller's supported position, an event dated before an entity's formation, circular direct ownership without an explanatory instrument, percentages that exceed their stated basis, a security class absent from the governing documents, a pledge without release evidence, a beneficial owner disconnected from the holding chain, or a closing instruction issued by a party with no supported authority.

Graph tests create exceptions rather than factual conclusions. A quantity mismatch may reflect a stock split, conversion, partial evidence or data-extraction error. The exception should route to the evidence owner with the exact claims and source locations that produced it.

5. EVIDENCE TAXONOMY AND SOURCE HIERARCHY

5.1 Source classes

The system needs a declared source hierarchy for each proposition. The authorised issuer register, register of members or transfer-agent record may govern registered ownership. Constitutional documents and executed agreements govern contractual rights subject to law and interpretation. Government registers and regulated identity sources can support entity status. Independent sanctions lists supply official screening data. Seller representations, broker summaries, platform records and analyst notes provide useful claims with different authority.

Source class	Examples	Typical use	Control
authoritative corporate record	issuer ledger, register of members, authorised transfer-agent confirmation	registered holder and position	verify controller, date, scope and authenticity
executed legal instrument	subscription agreement, transfer deed, purchase agreement, SPV agreement, pledge or release	event, rights, obligations and conditions	preserve complete signed version and specialist interpretation
constitutional or governance record	charter, bylaws, operating agreement, resolutions, consents	authority, class rights and approval	confirm current version and relevant entity
official registry	company register, good-standing record, PSC or beneficial-owner filing	identity, status and filed control data	retain retrieval date and jurisdictional limitation
official compliance source	UN and OFAC sanctions data	names, identifiers and programme data	use current machine-readable source and match resolution [18-22]
independent service evidence	administrator, auditor, custodian, escrow or counsel confirmation	service-controlled fact	authenticate sender, scope and reliance language
counterparty representation	questionnaire, certificate, warranty, email	represented fact	label representation and test against higher-authority evidence
intermediary or platform record	transaction summary, account statement, marketplace workflow	intake and coordination	identify role, limitations and underlying source
analyst work product	chronology, graph, score, memo	derived analysis	cite all inputs, method, reviewer and version

5.2 Authenticity and completeness

An authentic document can still be incomplete, superseded or irrelevant. The ingestion process should preserve the original file, cryptographic hash, receipt channel, supplier, access classification and processing history. It should detect missing pages, unreadable scans, broken signatures, inconsistent pagination, attachments referenced but absent, and schedules omitted from the data room. Digital-signature validation and trusted delivery channels can provide additional evidence where available.

Document status matters. A draft, specimen, execution copy, conformed copy, extract and certified copy should not share one undifferentiated label. The system should avoid inferring execution from a filename. It should compare signature pages, dates, parties, defined terms and schedules and route discrepancies.

5.3 Claim schema

Field	Purpose
claim ID	stable reference for review and release
subject, predicate, object	machine-readable proposition
plain-language statement	reviewable wording
source ID and exact location	inspection path to evidence
source authority and evidence class	hierarchy and provenance
valid from and valid to	real-world period asserted
recorded at	system observation time
extraction method and version	parser or analyst provenance
confidence	extraction or resolution confidence, not truth probability
conflict status	none, candidate conflict, confirmed conflict or resolved

Field	Purpose
permission and purpose	allowed users and use
reviewer and decision	accountable acceptance, rejection or condition
expiry or refresh trigger	staleness control

5.4 Negative evidence

Absence should be recorded carefully. A search that did not locate a pledge is not evidence that no pledge exists. The record should state the population searched, query or procedure, date, operator and limitations. A negative confirmation from an authorised party carries a different evidential weight. The system should use language such as “no responsive item found in the reviewed population” and avoid converting it into “no encumbrance exists”.

6. THE DATA ROOM AS AN EVIDENCE SYSTEM

6.1 Requirements matrix

A transaction data room should be generated from a requirements matrix rather than treated as an arbitrary upload folder. Each requirement links to an item, a claim or an explicit exception. Requirements vary by direct share or SPV structure, jurisdiction, security, buyer, seller and settlement method. The matrix should be versioned and approved by the responsible transaction and legal teams.

Core domains include entity formation and good standing; ownership registers and capitalisation; governing documents; security rights; acquisition and prior-transfer instruments; board, shareholder, manager, member or partner approvals; transfer restrictions and notices; beneficial ownership and authority; KYC, AML and sanctions; encumbrances; financial and tax evidence; fees and waterfalls; service-provider confirmations; information rights; litigation and disputes; payment instructions; settlement deliverables; and post-closing record updates.

6.2 Permission classes

The file population can contain personal data, confidential issuer information, bank details, signatures, tax records, privileged legal analysis and commercially sensitive terms. Permissions should apply before retrieval. A user who cannot access a source should not receive an answer derived from it. The index should therefore carry transaction, entity, document class, recipient, purpose, jurisdiction, privilege and field-level labels as required.

Redaction should produce a separate derivative with its own hash, purpose, creator and link to the original. The system should record which version was disclosed to which recipient. A model provider's product controls do not replace the user's access architecture or contractual assessment.

6.3 Freshness and event triggers

Closing readiness changes when a new transfer, lien, consent, ownership change, sanctions update, issuer action or document amendment occurs. The data room needs scheduled reviews and event-driven refresh. Each material claim should point to a source owner and refresh trigger. A last-updated banner without claim-level dates is insufficient.

6.4 Release bundles

A release bundle should be immutable after approval and should contain the exact disclosed files, derived memo, graph snapshot, exception register, approval record and recipient permissions. The bundle's manifest should list hashes and versions. If a correction is required, the system should create a superseding release and preserve the earlier one. This approach supports later reconstruction of what the buyer, intermediary, counsel and settlement parties actually saw.

7. DOCUMENT-EXTRACTION PIPELINE

7.1 Ingestion and preservation

The pipeline begins with controlled receipt. Files are quarantined, malware-screened, hashed and assigned a stable ID. Native text, scanned pages, spreadsheets, email containers and image formats follow different parsing paths. The original remains unchanged. A processed derivative records the tool, version, configuration and timestamp that produced it.

OCR output should preserve page coordinates and confidence. Tables require row and column structure. Handwritten or low-resolution annotations should route to manual review. Password-protected, corrupt, truncated and unsupported files should produce explicit exceptions. The system should also recognise documents embedded as attachments or portfolios where the toolchain supports them.

7.2 Classification and segmentation

Classification should identify document type, entity, transaction, status, parties, governing law, language and confidentiality. Long documents should be segmented along clauses, schedules, tables, signature blocks and defined-term relationships. A share-purchase agreement cannot be reliably reviewed as isolated fixed-length text chunks because the meaning of a clause often depends on definitions, exceptions and schedules.

The index should retain document hierarchy and cross-references. When a model receives clause 7.2, it may also need the defined terms, annexed security schedule and clause 7.5 exception. Retrieval should therefore support linked expansion within a bounded and reviewable context.

7.3 Structured extraction

The extraction schema should be narrow and explicit. A party object might contain printed name, legal role, capacity, address, identifier, signature status and source span. A restriction object might contain affected security, restricted act, trigger, beneficiary, notice, period, waiver authority, consent authority, exceptions and source spans. The system should permit “unknown”, “not stated” and “ambiguous” values. Forced completion increases the chance of invented fields.

7.4 Deterministic validation

After extraction, deterministic checks compare dates, quantities, currency, legal names, identifiers, signatures, totals and cross-references. A parser can detect that a schedule totals 98,000 shares while the purchase agreement states 100,000. It should not silently reconcile the difference. A validator can also identify an unsigned signature block, a defined term with no definition, or a referenced consent absent from the room.

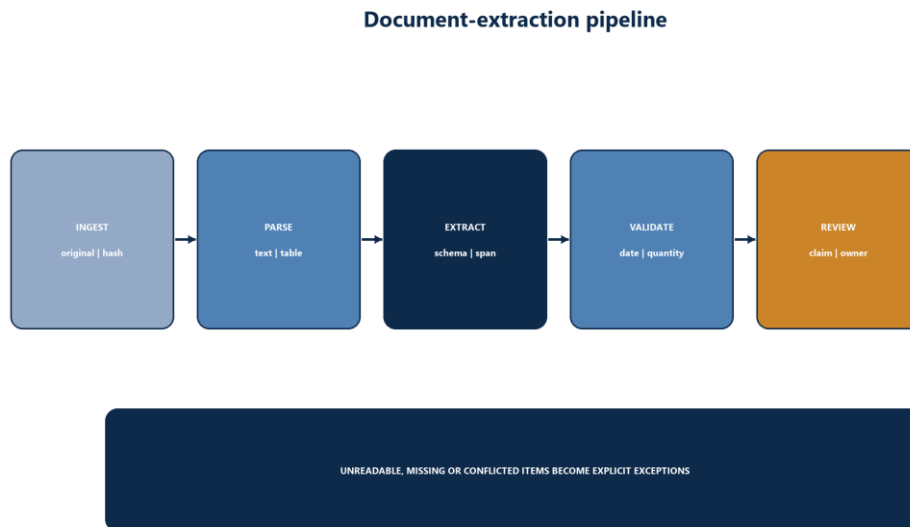


Figure 4. Document-extraction pipeline from immutable source to reviewed claim

Source: Matchpoint evidence architecture; Claude product context [23-26].

Stage	Output	Gate
receipt	original, hash, supplier and access label	accepted channel and malware result

Stage	Output	Gate
parse	text, tables, images and coordinates	completeness and quality checks
classify	document type, entity, status and confidentiality	reviewer confirmation for material items
extract	schema objects with exact source spans	field confidence and required-null policy
validate	deterministic inconsistencies and missing dependencies	zero suppressed exceptions
review	accepted, rejected or conditioned claims	named reviewer with authority
publish	graph and release-ready evidence	version, permission and audit record

8. ENTITY RESOLUTION AND BENEFICIAL-OWNERSHIP GRAPH

8.1 Candidate generation

Candidate generation combines normalised names, transliteration, aliases, historical names, jurisdictions, addresses, incorporation dates and identifiers. Corporate suffixes should be normalised without discarding the source form. Person matching should be handled in a restricted service with lawful purpose, data minimisation and appropriate security.

The candidate stage can use fuzzy similarity and embeddings to find possible matches. It should favour recall and explain why a candidate appeared. Exact or corroborated identifiers then drive higher-confidence resolution. A model-generated statement that two entities “look the same” is insufficient.

8.2 Resolution decision

Resolution state	Meaning	Permitted downstream use
exact identifier match	same durable identifier under compatible jurisdiction	link subject to source and validity review
corroborated match	several independent attributes agree and no material conflict	reviewer can approve link
probable candidate	similarity exists with incomplete corroboration	exception and investigation only
conflicted	identifiers or material attributes disagree	block aggregation and route review
distinct	reviewer determines separate identities	preserve anti-link evidence

Every manual merge and split should be reversible and logged. The system should explain which claims depend on an identity link because changing the link may alter ownership totals, sanctions exposure and authority.

8.3 Ownership and control paths

Beneficial ownership is represented as a path, not one percentage field. The graph records direct holdings, indirect holdings, voting control, appointment rights, contractual control, nominee relationships and other applicable bases. Percentage calculations should state the denominator, class, date and multiplication method. Threshold analysis should be parameterised by jurisdiction and policy and reviewed by compliance.

FATF guidance emphasises access to adequate, accurate and up-to-date beneficial-ownership information [10]. UAE rules include verification through reliable and independent sources [11-13]. Official filings can inform the analysis while remaining subject to their jurisdictional definitions and update cycles. The system should not treat one registry field as universal proof.

8.4 Provenance model

PROV-O's entity, activity and agent concepts provide a useful foundation [28]. A source document is an entity. OCR and extraction are activities. A claim is derived from a source span. A software agent and human reviewer participate in activities. A released memo is derived from reviewed claims. This makes the audit trail explicit and supports questions such as which model version, source and reviewer contributed to a material conclusion.

Entity-resolution and provenance architecture**Figure 5. Entity-resolution and provenance architecture**

Source: Matchpoint architecture; GLEIF, BODS and W3C context [14-17,28,32].

9. TRANSFER-RESTRICTION AND RIGHTS ENGINE

9.1 Clause taxonomy

Private-security transfers can be affected by restrictions in charters, bylaws, shareholder agreements, investor-rights agreements, stock plans, purchase agreements, side letters, SPV agreements and applicable law. A usable taxonomy includes issuer consent, board approval, manager or general-partner consent, rights of first refusal, rights of first offer, co-sale rights, tag-along and drag-along rights, lock-ups, permitted-transferee conditions, competitor restrictions, minimum-transfer sizes, accredited or qualified investor requirements, securities-law conditions, information-access conditions and indirect-transfer or change-of-control provisions.

The engine should extract the operative clause, defined terms, exceptions, affected security, triggering transaction, notice method, notice period, election period, required information, waiver authority, consequences and source locations. It should link cross-references and amendments. It must preserve ambiguous drafting for counsel review.

9.2 Rule representation

A rule can be represented as a decision table with inputs, tests, outputs and missing-evidence states. For example, a right-of-first-refusal workflow may require proposed transferee identity, price, payment form, quantity, notice date and delivery evidence. The system can calculate a contractual deadline only after counsel or an authorised legal rule owner confirms the operative clause, calendar convention and trigger date.

Rule component	Example representation
scope	direct or indirect transfer of defined securities by a covered holder
trigger	proposed sale to a non-permitted transferee
input facts	holder, buyer, security, quantity, price, terms, notice delivery
required action	deliver notice with specified information
decision party	issuer, company designee or rights holder as stated
time window	clause-derived period with calendar convention
evidence	notice, delivery receipt, election, waiver or lapse confirmation
unresolved state	missing amendment, ambiguous definition or unconfirmed delivery

9.3 Direct and indirect transfers

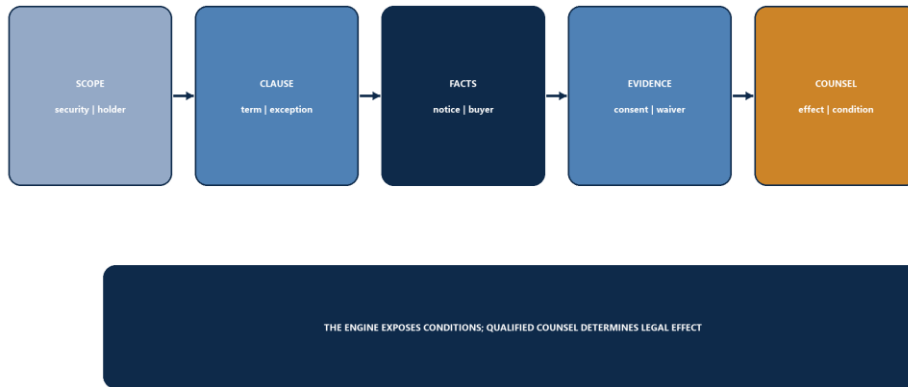
An SPV sale may be described commercially as an entity-interest transfer rather than a share transfer. The governing documents may nonetheless contain indirect-transfer, change-of-control or beneficial-ownership provisions. The graph should therefore connect the proposed transaction at the SPV layer to downstream securities and query clauses that reference indirect disposition or control. Counsel determines applicability.

9.4 Securities-law route

SEC guidance states that private-secondary transactions require registration or an exemption [1]. Rule 144 and Section 4(a)(7) have their own conditions [4-5]. The system should create a route object that lists the proposed exemption, facts required, evidence, counsel owner and unresolved conditions. It should avoid describing a resale as “compliant” solely because the parties are accredited or the issuer is private.

9.5 Output language

The engine's output should use bounded language: “clause located”, “fact supported”, “condition appears triggered for counsel review”, “waiver supplied”, “delivery unverified”, or “legal effect determined by counsel”. It should cite exact spans. A green status means the configured review gate has been completed; it does not guarantee enforceability or title.

Transfer-restriction decision flow**Figure 6. Transfer-restriction decision flow**

Source: Matchpoint clause-control framework; US legal context [1-6].

10. COUNTERPARTY, AML AND SANCTIONS TRIAGE

10.1 Identity before scoring

Counterparty triage begins after identity resolution. The system should identify the seller, buyer, introducing party, signatories, beneficial owners, controllers, payment recipient and settlement agents. It should preserve each party's legal role and authority. A recognised brand, platform account or business email does not establish that the contracting and receiving entities are the same.

Sanctions screening should use current official sources and a controlled resolution process. The United Nations maintains a consolidated list for Security Council sanctions measures [18]. OFAC publishes sanctions-list search and data services, guidance and ownership-related interpretations [19-22]. A name similarity produces a candidate match. Compliance reviewers need identifiers, ownership paths, programme context and applicable-law analysis to resolve it.

10.2 Authority and payment controls

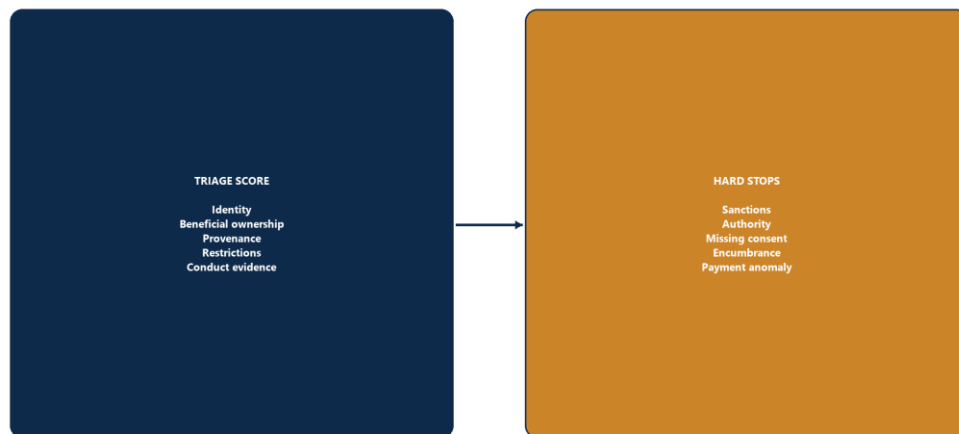
Authority should be evidenced through governing documents, resolutions, powers, incumbency, authorised-signatory records and specialist confirmation as appropriate. The system should compare the contracting party, registered holder, beneficial owner, invoice issuer and bank-account beneficiary. A mismatch requires explanation and approval. Changes to payment instructions should trigger out-of-band verification with a previously validated contact and segregation of duties.

Payment risk is distinct from title risk. Escrow, custodian, transfer-agent and delivery-versus-payment structures can reduce operational exposure depending on their terms and controls. The diligence system records the selected settlement mechanism and required release conditions. It does not assume a service provider guarantees the transaction.

10.3 Transparent triage rubric

The score is an exception-prioritisation tool. It should never conceal a blocking rule. A confirmed sanctions prohibition, unresolved identity, unsupported authority or payment-instruction anomaly may create a hard stop regardless of the aggregate score. Weights and thresholds should be approved by the relevant compliance and transaction authorities and tested against historical cases.

Domain	Example evidence	Example exception	Gate type
legal identity	registry, identifier, formation evidence	incompatible identifier	hard stop until resolved
beneficial ownership	ownership graph, declarations, official sources	unexplained owner or threshold path	compliance review
sanctions	official list data and match record	unresolved candidate or owned entity	hard stop or specialist decision
authority	resolutions, power, signatory evidence	signatory absent or scope unclear	hard stop until supported
provenance	ledger, instruments and event graph	missing prior transfer or quantity gap	transaction and legal review
restrictions	clauses, notices, consents and waivers	condition unmet or applicability unclear	legal closing condition
encumbrances	pledge, filing, release and confirmation	unreleased security interest	legal and settlement condition
payment	beneficiary and verified instructions	last-minute change or third-party payee	finance hard stop
conduct evidence	verified litigation, regulatory or fraud evidence	material unresolved allegation	risk committee review

Counterparty risk rubric with hard-stop overlays**Figure 7. Counterparty-risk rubric with hard-stop overlays**

Source: Matchpoint triage framework; beneficial-ownership and sanctions context [10-13,18-22,27].

10.4 Adverse-information boundaries

Open-source adverse-information analysis can introduce false matches, outdated reports and legally sensitive personal data. Searches should use an approved purpose, documented sources, date and identity-resolution method. The system should distinguish allegation, proceeding, finding, sanction and conviction. Material findings need qualified compliance or legal review. Generated summaries should cite the underlying source and avoid amplifying unsupported allegations.

11. CLAUDE, RETRIEVAL AND KNOWLEDGE-GRAPH ARCHITECTURE

11.1 Bounded role for Claude

Claude can support document classification, structured extraction, clause comparison, exception explanation, question answering and draft memoranda. Anthropic's citation capability can return source-linked answers from supplied documents [23]. Its PDF processing can use text and page images subject to current product limits and configuration [24]. These capabilities support inspection; they do not establish source authenticity, legal sufficiency or factual truth.

The architecture should place Claude between a permission-aware retrieval service and a structured validation layer. The model receives the exact task, approved source passages, graph facts, unresolved exceptions, recipient, output schema and abstention rules. It returns structured claims with citations and status. Deterministic services then check identifiers, numbers, dates, source permissions, required fields and citation locations before human review.

11.2 Architecture layers

Layer	Function	Minimum control
source systems	data room, registers, agreements, KYC and transaction records	owner, version, access class, hash and retention
ingestion	preserve, scan, parse, OCR and classify	immutable original and processing log
evidence store	text, tables, coordinates, objects and source hierarchy	exact location and permission inheritance
knowledge graph	entities, instruments, claims, events, ownership and approvals	bi-temporal provenance and reversible resolution
retrieval	graph query, lexical search, vector search and linked-context expansion	permission before retrieval, source authority and bounded context
Claude	extract, compare, explain and draft	explicit schema, citations, abstention and prompt-injection boundary
deterministic rules	quantities, dates, graph invariants, restriction rules and payment checks	versioned rule owner and reproducible result
workflow	exception queue, specialist review, approvals and release	segregation of duties and immutable decision record
monitoring	access, model, retrieval, quality, exceptions, cost and incidents	threshold, alert, rollback and periodic review

11.3 Retrieval by authority and relationship

Similarity alone can retrieve a convenient clause from a superseded document. Retrieval should first constrain transaction, entity, document status, permission and effective period, then rank by source authority and relevance. Graph traversal can pull the amendment, defined terms, schedules and approval linked to a clause. Hybrid lexical and semantic retrieval can then identify supporting spans.

Queries should state the proposition being tested. “Who owns the shares?” is too broad. A controlled query might ask: “Which approved sources identify the registered holder of 25,000 Series C shares as of the proposed closing date, and are there conflicting quantities or later transfer events?” The answer should separate record evidence, representations and unresolved claims.

11.4 Prompt contract

A system prompt should establish role, task, allowed sources, output schema, citation requirement, prohibited inference, ambiguity handling and escalation. Documents are untrusted content. Instructions within a document should be treated as evidence text and never as system commands. Anthropic's guardrail guidance includes measures for jailbreak and prompt-injection risk [25]. The application should also isolate tools, restrict actions, validate outputs and test adversarial cases.

11.5 Model and configuration record

Every material run should record model identifier, provider, date, system prompt version, tool configuration, retrieval query, source IDs, token or context limits, output and validation result. The release does not need to expose sensitive internal configuration to every recipient. The internal audit trail must permit reconstruction and comparison after a model or prompt change.

12. CITATION AND CLAIMS MODEL

12.1 Citation presence and citation support

A citation proves that an answer points somewhere. Review must establish that the cited passage supports the exact proposition, applies to the correct entity and period, is authoritative for the use, and may be disclosed to the recipient. Anthropic's current documentation describes source locations for citations and notes product constraints [23]. The application should store both the model-provided location and its own immutable source reference.

12.2 Atomic claims

Compound sentences create ambiguous support. A statement such as “Seller A owns 25,000 shares, has authority to sell them and no consent is required” contains at least three propositions. Each proposition should have its own citations, evidence class and reviewer. The narrative generator can recombine approved atomic claims for readability after validation.

Test	Reviewer question	Failure response
source identity	Is this the intended version and entity?	block and retrieve the authoritative source
exact support	Does the span entail the whole atomic claim?	narrow, correct or reject the claim
temporal fit	Was the source effective for the relevant date?	retrieve current or event-specific evidence
authority	Can this source establish the proposition?	relabel representation or seek stronger evidence
completeness	Do definitions, schedules or exceptions change the meaning?	expand context and re-review
permission	May this source inform this recipient and purpose?	remove context and route disclosure approval
conflict	Is there a materially inconsistent claim?	display both and assign resolution owner

12.3 Conflict sets

The system groups claims that address the same proposition and time. Compatible claims can reinforce a conclusion; incompatible claims create a conflict set. A conflict is resolved through a recorded decision that identifies the accepted operating claim, rejected or superseded claims, reason, authority and effective date. Historical claims remain visible.

12.4 Human determination objects

Specialist conclusions should also be structured. A counsel determination records the precise issue, reviewed population, applicable jurisdiction, conclusion, conditions, limitations, date and authorised person. A compliance resolution records candidate matches, identifiers, ownership analysis, programme or rule, disposition and reviewer. The system should not paraphrase those determinations beyond their approved scope.

13. WORKFLOW FROM DATA ROOM TO SETTLEMENT

13.1 Intake and mandate boundary

The transaction owner records the proposed asset, quantity, structure, parties, roles, jurisdiction, commercial terms, timeline and intended settlement route. A9 intermediaries record their engagement and permitted activity. A8 buyers record their approval process and advisers. The system creates a transaction ID and a requirements matrix based on the approved template.

13.2 Evidence collection

The seller or authorised source supplies documents through controlled channels. Each requirement is linked to a supplied item, a reasoned not-applicable determination or an open request. The system preserves originals, classifies access and routes material documents for source-owner confirmation. Automated extraction can begin while incomplete and conflicting items remain visibly open.

13.3 Graph construction and exceptions

Entity resolution joins parties and SPVs. Structured extractions create candidate claims and events. Graph invariants test dates, quantities and links. The restriction engine locates potentially applicable clauses. Beneficial-ownership and sanctions services evaluate the approved identity population. Every exception has an owner, severity, due date, evidence links and resolution state.

13.4 Specialist determinations

Qualified counsel addresses title, transfer restrictions, enforceability, securities-law route and transaction documents as applicable. Compliance resolves KYC, beneficial-ownership and sanctions matters. Tax, accounting and regulatory specialists address their domains. Issuer or authorised transfer-agent evidence confirms record and process requirements. The system records decisions without expanding their scope.

13.5 Investment and transaction approval

The investment committee receives the commercial underwriting, chain graph, evidence summary, risk rubric, specialist determinations, unresolved conditions, downside scenarios and proposed closing controls. Approval should state any conditions precedent, delegated authorities and expiry. A positive investment decision does not release payment.

13.6 Closing and settlement

The closing checklist links each condition to evidence and approval. Payment instructions pass a separate verification workflow. Where used, escrow, custodian or transfer-agent steps are recorded. The release authority confirms conditions, instructions and segregation. Post-closing evidence includes updated issuer or SPV records, executed instruments, receipts and final allocation. The graph receives a new event rather than overwriting the proposed event.

13.7 Post-closing monitoring

If the investment remains in an SPV, subsequent transfers, fees, distributions, corporate actions, amendments and ownership changes can affect the position. The evidence system should continue under an approved monitoring scope. Access and retention rules should reflect closed-transaction and investor obligations.

14. WORKED VERIFICATION EXAMPLE

14.1 Scenario facts

[Unverified illustrative scenario] A family office, Buyer FO, is considering a USD 4.8 million purchase of all membership interests in Alpha Access SPV II LLC. The SPV is represented to hold 100,000 Series D preferred shares in Nova Systems, Inc. The seller, Seller Holdings Ltd, holds its SPV interest through a nominee. An A9 intermediary has introduced the parties. All names, values, documents, dates and thresholds in this scenario are invented for method illustration and do not describe a Matchpoint or client transaction.

The room contains an issuer certificate in the SPV's name for 100,000 shares, an issuer cap-table export showing 98,000 shares, the SPV operating agreement, a prior membership-interest assignment, a nominee declaration, a board consent, a purchase agreement draft and an email with payment instructions. The issuer shareholder agreement contains a right of first refusal over direct and certain indirect transfers. The SPV operating agreement requires manager consent for a transfer of membership interests.

14.2 Extraction output

[Unverified illustrative scenario] The pipeline identifies five entities, two individuals, three instruments, one security class, two proposed transfer events and four approval objects. OCR confidence is low on one certificate digit. The quantity validator detects a 2,000-share difference between the certificate and cap-table export. The signature validator marks the prior assignment complete but finds no manager consent attached. The payment comparator finds that the beneficiary name differs from the contracting seller.

14.3 Graph and restriction analysis

[Unverified illustrative scenario] The graph connects Buyer FO to the proposed SPV-interest acquisition and the SPV to two conflicting issuer-position claims. It records the nominee as registered holder of the seller interest and Seller Holdings as represented beneficial owner. The engine flags the shareholder-agreement indirect-transfer clause for counsel review, identifies the SPV manager-consent requirement and creates an unresolved authority exception for the signatory.

14.4 Counterparty triage

[Unverified illustrative scenario] Official sanctions screening produces no resolved match for the supplied identifiers; the record states the sources, time and reviewer and does not claim that sanctions risk is absent. The third-party payment beneficiary creates a finance hard stop. Compliance requests beneficial-ownership evidence for Seller Holdings and the payment recipient. The intermediary's role is recorded as introduction and coordination; no title or compliance verification is attributed to it.

14.5 Resolution and release

[Unverified illustrative scenario] The issuer supplies a dated ledger extract supporting 98,000 shares and explains that 2,000 shares were cancelled after a repurchase. The original certificate is superseded and cancellation evidence is added. Counsel records that manager consent is required and separately addresses the indirect-transfer clause. The SPV manager executes a consent. The seller replaces the payment instruction with an account in its verified legal name, and finance confirms it through an approved channel.

The investment committee receives a revised exposure schedule based on 98,000 underlying shares, updated commercial economics, the resolved graph, counsel determinations and closing conditions. The closing controller releases funds only after executed purchase documents, consent, verified instructions and the agreed settlement mechanism are complete. The system then records the post-closing member register and final issuer-position evidence.

Worked verification example**Figure 8. Worked chain-of-title verification example**

Source: Matchpoint framework. All names, values and events are unverified illustrative assumptions.

14.6 Lessons

The scenario demonstrates why a polished certificate or contract should not dominate conflicting authoritative evidence. It also shows that quantity, authority, restriction and payment exceptions require separate owners. The graph makes their dependencies visible. The aggregate score cannot override a finance hard stop or legal closing condition.

15. RISK-SCORING RUBRIC AND RELEASE GATES

15.1 Four outputs

The system should produce four distinct outputs: an extraction-quality score, an evidence-coverage score, a counterparty-triage score and a release-gate status. Extraction quality describes parser performance. Evidence coverage describes whether required propositions have approved support. Counterparty triage prioritises review. Release status reflects completion of configured mandatory decisions. Combining all four into one number obscures risk.

15.2 Illustrative score design

[Unverified illustrative scenario] The following weights are a design example requiring management, legal and compliance approval before use.

Triage domain	Illustrative weight	Example scoring basis
identity and beneficial ownership	20	identifier corroboration, ownership coverage and unresolved links
authority	15	signatory, governing authority and scope evidence
provenance	20	supported position, event continuity and quantity reconciliation
restrictions and approvals	15	clause coverage, notices, consents and specialist determination
sanctions and compliance	15	current screening, ownership analysis and match resolution
encumbrance and adverse evidence	5	searches, representations and release evidence
payment and settlement	10	beneficiary match, instruction verification and settlement controls
Total	100	triage only; hard stops remain separate

[Unverified illustrative scenario] A low-risk band might require a score below 20 with no hard stop, medium 20 to 39, high 40 to 59 and critical 60 or above. These thresholds have no empirical validation in this paper. They should be calibrated on an approved labelled case set and may be unsuitable for a particular organisation or jurisdiction.

15.3 Hard-stop register

Hard-stop candidate	Required release authority
unresolved contracting-party identity	compliance and transaction authority
unresolved sanctions prohibition or ownership issue	qualified compliance or legal authority
unsupported seller authority	qualified counsel and transaction authority
material break in provenance	qualified counsel, issuer or record authority and investment committee
required consent or waiver absent	qualified counsel and named consent authority
unresolved encumbrance affecting transfer	qualified counsel and settlement authority
unverified or changed payment instruction	finance or settlement authority
retrieval of impermissible or privileged source	information owner, privacy or legal authority

15.4 Release decision

A release gate records “pass”, “pass with named conditions”, “fail” or “expired”. A pass confirms completion of the configured process at that time. It does not guarantee title, legality, solvency, future performance or freedom from fraud. The release should list scope, sources, material assumptions, specialist determinations and residual conditions.

16. GOLDEN-SET EVALUATION

16.1 Evaluation population

Anthropic's evaluation guidance recommends task-specific tests and clearly defined success criteria [26]. T32 should use a golden set of de-identified or synthetic documents and cases approved for the environment. It should represent clean native PDFs, difficult scans, tables, amendments, stacked entities, nominee relationships, conflicting quantities, indirect-transfer clauses, sanctions name collisions, payment changes and prompt-injection attempts.

The set should contain labels from authorised legal, compliance and transaction experts. It should separate extractable fields from determinations requiring judgement. Changes to models, prompts, parsing, retrieval, rules or schemas should run against the same versioned set before release.

16.2 Metrics

Component	Primary metric	Release concern
classification	precision and recall by material document class	critical class missed
field extraction	exact match or approved tolerance	identifier, quantity, date or party error
table extraction	cell and structural accuracy	detached headers or wrong totals
entity resolution	pairwise precision and recall	false merge has high consequence
relationship extraction	typed-edge precision and recall	wrong owner, authority or instrument link
retrieval	evidence recall at reviewed context size	authoritative clause omitted
citation	claim support and exact location accuracy	unsupported material proposition
rule engine	agreement with approved test outcomes	missed hard stop or false clearance
abstention	appropriate abstention rate	confident answer under absent or conflicting evidence
workflow	exception routing and approval integrity	decision bypass or unauthorised release

16.3 Severity-weighted errors

An error involving punctuation and an error involving the identity of the registered holder should not carry equal weight. The test plan should define severity by potential consequence and route critical errors to zero-tolerance or explicit waiver. False merges, missed restrictions, incorrect quantities, unsupported authority and payment mismatches deserve elevated severity.

16.4 Adversarial tests

Documents should include text instructing the model to ignore the workflow, fabricate a consent or disclose restricted information. The application should prove that document content cannot change system authority. Tests should also cover malicious filenames, hidden text, Unicode confusion, contradictory attachments, oversized documents and tool-call attempts. NIST's Generative AI Profile identifies risk-management actions for generative systems [30]; NIST's Secure Software Development Framework provides a broader secure-development discipline [31].

16.5 Production monitoring

Production monitoring should sample material claims, track reviewer corrections, measure unresolved exceptions, detect distribution shifts and record access events. A rise in manual corrections after a model update should trigger rollback or investigation. User acceptance alone is not proof of correctness. Reviewer workload, elapsed time and correction rate should be observed against an approved baseline.

17. SECURITY, PRIVACY AND GOVERNANCE

17.1 Data classification and minimisation

The evidence population may contain confidential issuer information, personal identifiers, bank details, signatures and privileged analysis. Collection and processing should have an approved purpose and legal basis. The system should minimise fields, segregate sensitive services, restrict exports and apply retention and deletion rules. The paper does not determine the applicable privacy regime for a transaction.

17.2 Access before retrieval

Identity and access controls should enforce least privilege, transaction isolation, recipient permissions and privileged-document handling. Permission checks occur before retrieval, model context construction and export. Logs should record source access, graph query, model use, review and disclosure. High-risk administrative actions should require stronger authentication and segregation.

17.3 Supplier and model governance

The organisation should assess provider terms, data use, retention, location, security, incident handling, sub-processors, model changes, availability and exit. Product settings and contractual commitments should be verified for the selected service and date. Sensitive use cases may require an API, private networking, regional controls or a different architecture. The system should avoid sending secrets that the approved design does not require.

17.4 Secure development

NIST SP 800-218 describes secure-development practices across preparing the organisation, protecting software, producing well-secured software and responding to vulnerabilities [31]. The T32 application should maintain a software bill of materials where appropriate, review dependencies, scan code and infrastructure, protect secrets, validate inputs and outputs, test authorisation, manage vulnerabilities and preserve a rollback path. Changes to rule sets and schemas deserve the same release discipline as application code.

17.5 AI risk governance

The NIST AI Risk Management Framework organises work around govern, map, measure and manage functions [29]. Its Generative AI Profile addresses risks specific to or amplified by generative AI [30]. Applied here, governance identifies accountable owners and risk tolerance; mapping defines parties, jurisdictions, data and consequences; measurement tests extraction, retrieval, citation and workflow; management sets release gates, monitoring and response.

17.6 Incident response

Incidents include unauthorised disclosure, incorrect release, model or rule failure, corrupted evidence, identity mis-resolution, sanctions-screening failure, payment fraud and supplier outage. The response plan should preserve evidence, stop affected workflows, identify impacted releases, notify accountable owners, correct or supersede outputs and document lessons. A released dossier needs a traceable recipient list so corrections can reach the right parties.

18. NINETY-DAY IMPLEMENTATION ROADMAP

18.1 Days 0 to 15: scope and evidence inventory

Select one transaction pattern, jurisdictional perimeter and accountable sponsor. Map A8 and A9 roles, legal and compliance authorities, data-room sources, settlement parties and current failure modes. Define the current process and baseline. Identify which determinations remain entirely outside the system.

Deliverables include a mandate boundary, RACI, data classification, document taxonomy, requirements matrix, claim schema, source hierarchy and approved golden-set plan. The team should also define prohibited data and tool actions.

18.2 Days 16 to 30: controlled ingestion and graph schema

Build immutable receipt, hashing, parsing, OCR and page-coordinate storage. Configure entity, security, instrument, event, claim, restriction and approval objects. Establish access labels before indexing. Load synthetic or approved de-identified cases and test reconstruction.

18.3 Days 31 to 45: extraction, resolution and rules

Implement narrow extraction schemas and deterministic validation. Add entity-resolution candidates and reversible reviewer decisions. Encode a small set of approved restriction rules and graph invariants. Integrate official sanctions sources through the organisation's approved screening process.

18.4 Days 46 to 60: Claude and cited analysis in shadow mode

Add permission-aware retrieval and Claude outputs with citations and abstention. Run alongside the current process without releasing model-assisted conclusions. Review every material field and claim. Record errors by severity and improve the source, schema, prompt or rule that caused them.

18.5 Days 61 to 75: bounded pilot

Pilot on a narrowly selected live or controlled case with explicit consent and full human authority. Use the exception queue, specialist determination objects and release bundle. Stop on critical error, access breach or workflow bypass. Compare elapsed time, reviewer effort, evidence coverage and correction rate with the approved baseline.

18.6 Days 76 to 90: decision and hardening

The governance body reviews evaluation evidence, security findings, specialist feedback, user behaviour, incidents, economics and residual risk. It may approve a bounded production scope, require remediation, extend shadow mode or stop. Any approved scope names transaction types, jurisdictions, data classes, models, rules, reviewers and release gates.

Ninety-day implementation roadmap

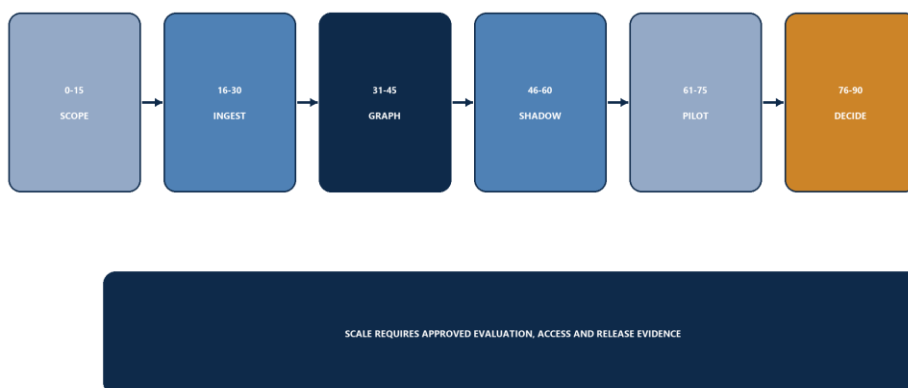


Figure 9. Ninety-day implementation roadmap

Source: Matchpoint implementation framework; AI and secure-development context [25-26,29-31].

18.7 Economics

The business case should distinguish implementation cost, ongoing software and specialist cost, review time, elapsed time, avoided rework, deal-throughput effects and loss events. Attributed Matchpoint or client revenue, cash cost reduction, loss reduction and alpha remain USD 0 in this paper because no approved observed evidence was supplied. Any productivity, conversion or loss-avoidance claim should state its baseline, period, counterfactual and finance approval.

19. RELEASE CHECKLIST AND CLAIMS REGISTER

19.1 Transaction release checklist

1. Confirm transaction ID, structure, parties, roles and governing jurisdictions.
2. Confirm issuer, security class, quantity, holder and proposed interest.
3. Reconcile the authoritative record, certificates and transaction instruments.
4. Reconstruct prior issuance and transfer events to the approved scope.
5. Resolve entity identities, aliases, nominees, custodians and beneficial owners.
6. Verify formation, status and authority evidence for each material entity.
7. Identify governing documents, amendments, side arrangements and current versions.
8. Review direct, indirect and change-of-control transfer restrictions.
9. Obtain and authenticate required notices, consents, waivers and approvals.
10. Record the proposed securities-law resale route and counsel determination.
11. Review encumbrances, pledges, liens and release evidence to the approved scope.
12. Complete KYC, beneficial-ownership, sanctions and adverse-information review.
13. Resolve signatory authority and contracting-party consistency.
14. Verify payment beneficiary and instructions through approved controls.
15. Confirm settlement mechanism, deliverables and segregation of duties.
16. Resolve all graph invariants and material extraction exceptions.
17. Validate every material claim, citation, period, source authority and permission.
18. Record specialist determinations with scope, date, conditions and limitations.
19. Present unresolved conditions and downside implications to the investment authority.
20. Freeze the approved release bundle, manifest, graph snapshot and exception register.
21. Release capital only under the separate authorised closing workflow.
22. Obtain post-closing instruments, register updates, receipts and final position evidence.

19.2 Public claims register

Claim	Evidence status in this paper	Permitted wording
LLMs can extract and compare private-market documents	supported as a technical capability subject to testing and controls [23-26]	AI-assisted extraction and cited analysis
citations establish title	unsupported	do not claim
a knowledge graph can represent provenance and ownership claims	supported as a design approach [14,16-17,28,32]	graph-based evidence and provenance model
the model can make legal determinations	unsupported	do not claim
the workflow prevents fraud or loss	unsupported	do not claim
the workflow guarantees a valid transfer	unsupported	do not claim
T32 proves cost saving, revenue, loss reduction or alpha	no approved observed evidence supplied	attributed amounts remain USD 0
the ninety-day plan fits every organisation	unverified implementation hypothesis	adapt and approve locally

19.3 Minimum operating pack

The production pack should include the approved architecture, source hierarchy, claim schema, graph schema, document taxonomy, requirements templates, rule catalogue, prompt and output contracts, golden set, evaluation report, access matrix, supplier assessment, incident plan, RACI, release checklist and change log. The transaction pack adds case-specific evidence and approvals.

20. LIMITATIONS AND CONCLUSION

20.1 Limitations

This paper does not provide legal, investment, regulatory, compliance, tax, accounting, privacy, cybersecurity or technical advice. It does not determine title or the validity of any transfer. It does not address every jurisdiction, security, entity form, exemption, contractual right, sanctions regime, insolvency issue, lien registry, tax consequence or regulated activity. Specialist advice and authoritative records remain essential.

The paper has not evaluated a production model on an approved labelled pre-IPO-secondary dataset. Product capabilities and official requirements can change. The worked scenario, score weights, thresholds, time plan and economics are unverified illustrative management assumptions. No client result is claimed. Author attribution to a named person remains pending CK approval; the organisation author is Matchpoint Partners.

Document authenticity can be attacked. Official registers can lag, contain errors or use definitions that differ from the transaction. A model can omit, misclassify or invent content. Entity resolution can merge different parties or split one party. Rules can encode an incomplete legal interpretation. Human reviewers can also err. The design reduces opacity by preserving sources, exceptions and decisions; it does not remove uncertainty.

20.2 Conclusion

AI-assisted chain-of-title diligence is best understood as an evidence-control system. Documents enter through a preserved and permissioned pipeline. Structured extraction creates candidate claims. Entity resolution and a knowledge graph connect issuers, securities, holders, beneficial owners, SPVs, instruments and events. Deterministic checks identify structural inconsistencies. Clause rules expose potentially applicable restrictions. Claude can help compare evidence and draft cited explanations. Named legal, compliance, issuer, investment, finance and settlement authorities make the consequential decisions.

For A8 family offices and UHNW buyers, the system offers a more inspectable route from commercial opportunity to executable ownership. For A9 intermediaries, it provides a clearer intake, disclosure and hand-off record. The most valuable output is not a confident narrative. It is a release pack in which every material proposition has a source, date, authority, permission, reviewer and unresolved-condition status before capital moves.

REFERENCES

- [1] U.S. Securities and Exchange Commission, “Private Secondary Markets,” updated 24 April 2026. <https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/private-secondary-markets>
- [2] Delaware General Assembly, Delaware Code Title 8, Chapter 1, Subchapter VI, sections 201-202, current online code. <https://www.delcode.delaware.gov/title8/c001/sc06/>
- [3] Delaware General Assembly, Delaware Code Title 8, Chapter 1, Subchapter V, section 159, current online code. <https://delcode.delaware.gov/title8/c001/sc05/index.html>
- [4] U.S. Securities and Exchange Commission, “Rule 144: Selling Restricted and Control Securities.” <https://www.sec.gov/reports/rule-144-selling-restricted-control-securities>
- [5] United States Code, 15 U.S.C. section 77d, including Section 4(a)(7). <https://www.law.cornell.edu/uscode/text/15/77d>
- [6] U.S. Securities and Exchange Commission, “Transfer Agents.” <https://www.sec.gov/about/divisions-offices/division-trading-markets/transfer-agents>
- [7] United Kingdom, Companies Act 2006, including register-of-members provisions. https://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf
- [8] UK Government, “People with significant control requirements” collection, updated 2026. <https://www.gov.uk/government/collections/people-with-significant-control-requirements>
- [9] UK Government, “Summary guidance for companies: register of people with significant control.” <https://www.gov.uk/government/publications/people-with-significant-control-summary-guidance/summary-guidance-for-companies-register-of-people-with-significant-control-pscs>
- [10] Financial Action Task Force, “Guidance on Beneficial Ownership of Legal Persons,” March 2023. <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>
- [11] United Arab Emirates, Cabinet Decision No. 109 of 2023 Regulating Beneficial Owner Procedures. <https://rulebook.centralbank.ae/en/rulebook/cabinet-decision-no-109-2023-regulating-beneficial-owner-procedures>
- [12] United Arab Emirates, Cabinet Resolution No. 134 of 2025 regarding the Executive Regulations of Federal Decree-Law No. 10. <https://rulebook.centralbank.ae/en/rulebook/cabinet-resolution-no-134-2025-regarding-executive-regulations-federal-decree-law-no-10>
- [13] Central Bank of the UAE, “Beneficial Ownership Identification and Verification.” <https://rulebook.centralbank.ae/en/rulebook/325-beneficial-ownership-identification-and-verification>
- [14] OpenOwnership, Beneficial Ownership Data Standard 0.4, “Key concepts.” <https://standard.openownership.org/en/latest/standard/concepts.html>
- [15] OpenOwnership, Beneficial Ownership Data Standard 0.4, “Representing nominees.” <https://standard.openownership.org/en/latest/standard/modelling/repr-nominations.html>
- [16] Global Legal Entity Identifier Foundation, “Level 2 Data: Who Owns Whom.” <https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-2-data-who-owns-whom>
- [17] Global Legal Entity Identifier Foundation, “Relationship Record CDF 2.1 Format.” <https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-2-data-relationship-record-rr-cdf-2-1-format>
- [18] United Nations Security Council, “United Nations Security Council Consolidated List.” <https://scsanctions.un.org/consolidated/>
- [19] U.S. Department of the Treasury, Office of Foreign Assets Control, “Sanctions List Search.” <https://ofac.treasury.gov/sanctions-list-search-tool>
- [20] U.S. Department of the Treasury, Office of Foreign Assets Control, “Other OFAC Sanctions Lists.” <https://ofac.treasury.gov/other-ofac-sanctions-lists>
- [21] U.S. Department of the Treasury, Office of Foreign Assets Control, “A Framework for OFAC Compliance Commitments,” May 2019. <https://ofac.treasury.gov/media/16331/download>
- [22] U.S. Department of the Treasury, Office of Foreign Assets Control, FAQ 585 on entities owned 50 percent or more. <https://ofac.treasury.gov/faqs/585>
- [23] Anthropic, Claude API Documentation, “Citations,” accessed 1 August 2026. <https://platform.claude.com/docs/en/build-with-claude/citations>
- [24] Anthropic, Claude API Documentation, “PDF support,” accessed 1 August 2026. <https://platform.claude.com/docs/en/build-with-claude/pdf-support>
- [25] Anthropic, Claude Documentation, “Mitigate jailbreaks and prompt injections,” accessed 1 August 2026. <https://platform.claude.com/docs/en/test-and-evaluate/strengthen-guardrails/mitigate-jailbreaks>
- [26] Anthropic, Claude Documentation, “Develop test cases,” accessed 1 August 2026. <https://platform.claude.com/docs/en/test-and-evaluate/develop-tests>
- [27] U.S. Department of the Treasury, Office of Foreign Assets Control, “Hash Values for OFAC Sanctions List Files.” <https://ofac.treasury.gov/specially-designated-nationals-list-sdn-list/hash-values-for-ofac-sanctions-list-files>
- [28] World Wide Web Consortium, “PROV-O: The PROV Ontology,” W3C Recommendation, 30 April 2013. <https://www.w3.org/TR/prov-o/>
- [29] National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework (AI RMF 1.0),” January 2023. <https://www.nist.gov/itl/ai-risk-management-framework>
- [30] National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile,” NIST AI 600-1, July 2024. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
- [31] National Institute of Standards and Technology, “Secure Software Development Framework (SSDF) Version 1.1,” NIST SP 800-218, February 2022. <https://csrc.nist.gov/pubs/sp/800/218/final>
- [32] World Wide Web Consortium, “RDF 1.1 Concepts and Abstract Syntax,” W3C Recommendation, 25 February 2014. <https://www.w3.org/TR/rdf-concepts/>

APPENDIX A. CLAIM RECORD TEMPLATE

Field	Entry
claim ID	stable transaction-specific identifier
proposition	one atomic statement
subject, predicate, object	graph representation
source	document ID, version, hash and exact location
evidence class	observed, represented, derived or determined
source authority	configured hierarchy for the proposition
valid period	real-world dates asserted
system time	receipt, extraction and decision timestamps
permission	transaction, recipient, purpose and restrictions
extraction	method, model or parser version and confidence
conflict	linked competing claims and status
reviewer	person, role, authority and date
disposition	accepted, rejected, conditioned or unresolved
refresh	expiry or triggering event

APPENDIX B. EXCEPTION RECORD TEMPLATE

Field	Entry
exception ID	stable identifier
transaction and entity	affected scope
type	identity, quantity, date, restriction, authority, sanctions, payment or other
severity	approved consequence scale
evidence	linked claims and exact source locations
description	bounded statement of the inconsistency or absence
owner	accountable resolver
required authority	specialist or approval body
due date	time-bound action
hard-stop state	yes, no or pending determination
resolution	action, evidence, decision and date
dependent claims	outputs requiring refresh after resolution

APPENDIX C. MODEL RUN RECORD

Field	Entry
run ID	immutable identifier
task	classification, extraction, comparison, answer or draft
model and provider	exact identifier and date
prompt and schema	versioned references
source population	permitted source IDs and versions
retrieval	query, filters and returned locations
output	structured response and citations
validation	deterministic checks and failures
reviewer	identity, role and disposition
release dependency	linked claims, memo or bundle