Broker Network Quality: Scoring Counterparties before Sharing a Live Block

A Global Permission, Evidence and Outcome Framework for Private-Market Intermediaries

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

Private-market transactions often depend on networks of brokers, introducers, placement agents, advisers and specialist intermediaries. A capable network can extend market access and execution capacity. A weakly controlled network can circulate duplicated inventory, exceed permissions, misstate authority, leak confidential information, obscure fees, create sanctions or fraud exposure, and consume time on opportunities that cannot settle. A contact list or relationship score does not provide an adequate basis for sharing a live block.

This paper develops a global permission, evidence and outcome framework for private-market intermediary networks. It establishes an entity-and-person master; verifies regulatory status, capacity and jurisdiction; confirms mandate and inventory authority; maps ownership, conflicts and complete economics; grades information permissions; measures communication conduct and operational readiness; records transaction and settlement outcomes; controls incidents and adverse information; applies evidence expiry and ongoing monitoring; and governs the decision to share, restrict, pause or refuse a live block. The framework includes six non-negotiable stop gates, a twelve-dimension scorecard, evidence tiers, a block-sharing protocol, event-based monitoring, a network portfolio dashboard, a ten-day diagnostic and a thirty-day implementation office.

The analysis draws on current official materials from the US Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Financial Conduct Authority, the Dubai Financial Services Authority and the Abu Dhabi Global Market Financial Services Regulatory Authority. Applicable requirements depend on the parties, activities, clients, security, capacity, communication, jurisdiction and transaction route. Current legal, regulatory, compliance, sanctions, data-protection, tax and accounting advice is required. Worked scores, thresholds, weights, time limits and scenarios are management assumptions used solely to demonstrate the framework.

JEL Classification: G12, G23, G24, G28, G32

Keywords: broker networks, counterparty due diligence, private markets, intermediary scoring, live blocks, mandate authority, settlement quality, transaction controls

1. Define network quality as permission, evidence and outcomes

Broker-network quality should answer a decision question: what may this counterparty receive, for which transaction, under whose authority, and with what evidence? Familiarity, responsiveness and claimed access can inform a relationship record. They do not establish identity, permission, mandate, inventory control or settlement capacity.

The network includes every firm and person that introduces, sources, markets, arranges, advises, places, warehouses, transfers or settles an opportunity. It can include regulated broker-dealers, investment firms, appointed representatives, corporate-finance advisers, finders, consultants, family-office principals, fund managers, issuer representatives and specialist transfer providers. The applicable capacity should be confirmed for the actual activity.

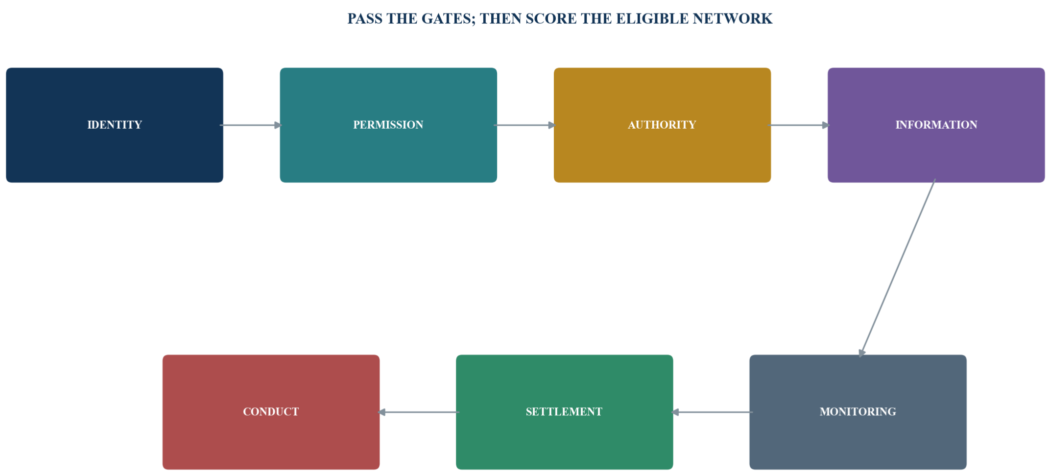
Quality has three layers. Permission covers legal entity, person, activity, jurisdiction, client type and communication route. Evidence covers mandate, authority, ownership, source lineage, contact authenticity, confidentiality, economics and transaction documents. Outcomes cover order quality, responsiveness, behaviour, funding, delivery, settlement, complaints and incident history.

A high total score cannot cure a failed stop gate. An unverified identity, missing permission, unauthorised representative, absent mandate, prohibited party or compromised communication channel should pause sharing regardless of relationship value. The score ranks eligible counterparties after the gates are passed.

The framework should operate at entity, person and relationship levels. A reputable firm can contain an individual without relevant authority. A qualified person can act outside the firm's permitted business. An authorised activity in one jurisdiction may not cover another route. The record should preserve these distinctions.

Decision owners need separation. A relationship owner supplies information and commercial context. A control owner verifies evidence and gates. A transaction owner decides the permitted sharing tier. Legal and compliance advisers determine reserved questions. The governing body approves policy, thresholds and exceptions.

Figure 1. Broker-network quality architecture



Applicable permissions and duties require transaction-specific advice.

2. Build an entity-and-person master before rating relationships

The master should identify the legal entity, trading names, registration number, jurisdiction, registered address, website, verified domains, official telephone numbers, ownership, controllers and group relationships. It links every representative to the entity for which that person claims to act.

Identity verification should use independent official sources. FINRA describes BrokerCheck as a free research tool whose firm and individual information draws from registration databases. The FCA describes its Financial Services Register as the official public record for authorised and previously authorised firms, individuals and other bodies. The DFSA and ADGM maintain public registers for their respective financial-services populations.

Contact verification needs its own control. A genuine firm name, regulatory reference number or website link can be copied by an impersonator. The FCA and DFSA have published warnings about cloned firms or cloned register pages. The reviewer should access the regulator through a known official domain and use independently retrieved contact details where confirmation is required.

The master should record the represented principal. FINRA Rule 2090 states that a member should know and retain essential facts about the customer and the authority of persons acting on the customer's behalf. The same operational question is valuable across the network: who authorised this person, for which activity, with what limits and until when?

Identifiers should remain stable across name changes, personnel moves and group reorganisations. A new email address or affiliated entity should create a relationship event rather than replace the historical record. Former affiliations remain visible with start and end dates.

Duplicate resolution matters. The same intermediary may appear under a personal brand, advisory company, regulated principal and special-purpose vehicle. The master should connect these records while preserving the distinct legal parties and capacities.

Table 1. Entity-and-person master

Record	Core fields	Independent evidence	Failure response
legal entity	name, number, address and status	official corporate or regulatory register	quarantine unresolved identity
regulated firm	permissions, restrictions and history	regulator's official register	restrict activity to confirmed scope
representative	name, role, employer and authority	firm confirmation and official record where available	pause person-level access
contact channel	domain, email, telephone and website	independently sourced contact details	block suspect channel
ownership	controllers and group relationships	official filings and declarations	escalate hidden or inconsistent control
relationship	introducer, client, counterparty or affiliate	engagement and internal records	resolve capacity before sharing

Verification sources and refresh periods should reflect the relevant jurisdiction and risk.

3. Verify permission for the actual activity and route

Regulatory status is a starting point. The file should test whether the firm and individual have the permissions required for the contemplated activity, client population, product and jurisdiction. A broad description such as advisory, brokerage or investment business can conceal material limits.

The activity map should describe what the intermediary will do: make an introduction, communicate an opportunity, solicit investors, recommend a security, arrange a transaction, transmit an order, negotiate terms, receive money, hold assets, operate a vehicle or advise a party. Each activity is mapped to the entity, person, location and represented client.

The US Securities and Exchange Commission explains that broker-dealer registration requirements can apply to persons engaged in securities transactions and points users to Investor.gov and BrokerCheck to verify licensing and registration. FINRA Rule 3110 requires member firms to maintain a supervisory system reasonably designed for compliance and expressly includes placement-agent and private-offering activity within its investment-banking examples.

The FCA's public guidance says that its Firm Checker can confirm whether a firm is authorised and has permission for the service sought. The Financial Services Register provides a fuller record, including restrictions and historical information. The FCA also advises checking the principal when an appointed representative may have exceeded the activities allowed by that principal.

Permission checks should use an as-of date and preserved evidence. Register status can change. A screenshot or export should identify the official source, URL, access time, entity, reference number, status, permissions, restrictions and reviewer.

Cross-border routes require specific analysis. The origin of a message, location of the recipient, security, investor type, issuer, intermediary capacity and method of solicitation can affect the assessment. Qualified advisers should determine the permitted route before live materials are shared.

4. Confirm mandate and inventory authority separately

An intermediary can be permitted to conduct an activity while lacking authority over the proposed block. The network file should therefore separate regulatory permission from transaction mandate and inventory evidence.

The mandate record identifies the principal, intermediary, issuer, security, class, quantity, price instruction, exclusivity, permitted recipients, jurisdictions, confidentiality, fees, term, withdrawal rights and settlement route. It records signatures, dates, governing law and verification with the principal where appropriate.

Inventory evidence should identify registered and beneficial owner, quantity, encumbrances, transfer restrictions, rights processes, issuer approvals, custodian or administrator records, and evidence date. Expected access, verbal supply, indicated interest and controlled inventory require different states.

Source lineage prevents duplication. A block repeated through several brokers can appear to create supply that does not exist. Each record should preserve the original holder, each intermediary hop, authority at every hop and evidence used to conclude that two offers are distinct or duplicated.

The live-block decision should set a permitted quantity and expiry. If the holder, mandate, security class, price, route or intermediary changes, approval reopens. A relationship owner's assurance cannot replace updated documents.

The firm should define language for incomplete inventory. A possible seller or exploratory discussion should be described accurately within restricted internal workflows. It should not enter external circulation as a live, owned, controlled or deliverable block.

5. Apply hard stop gates before a weighted score

The stop gates protect decisions that should not be averaged away. Six gates cover identity and channel authenticity; required permission and capacity; representative authority; mandate and inventory control; sanctions, financial-crime and prohibited-party checks; and confidentiality plus information permission.

A failed gate produces a defined state: reject, quarantine, restrict, investigate or obtain specialist approval. The policy should specify who can close the issue, what evidence is required and how long the closure remains valid. Commercial seniority should not create an override path outside the approved governance process.

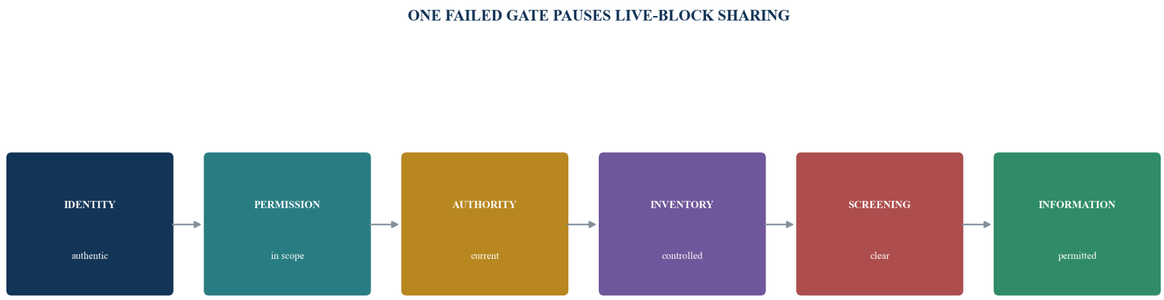
Identity failure includes an entity that cannot be independently resolved, a mismatched domain, a telephone number supplied only by the contact, an altered register link or an unexplained change in payment instructions. Permission failure includes absent, inactive, restricted or irrelevant authorisation where permission is required.

Authority failure covers a person who cannot be connected to the principal or regulated firm for the activity. Inventory failure includes missing owner evidence, inconsistent quantity, expired mandate, unknown encumbrance or broken source lineage. Financial-crime failure includes an unresolved sanctions match, opaque control or payment route that cannot pass policy.

Information failure covers missing confidentiality commitments, an unauthorised onward-sharing request, personal-channel use contrary to policy or a request for data beyond the approved tier. These failures can harm the issuer, seller and investors even if the counterparty later proves able to transact.

The gate log should show facts, sources, reviewer, status, decision, conditions, expiry and linked incident. A reviewer should be able to understand why access was granted without relying on the relationship owner's recollection.

Figure 2. Six-gate live-block decision



Gate outcomes are author-framework controls; applicable law and policy determine the final decision.

6. Score twelve dimensions after eligibility is established

Eligible counterparties can be scored across twelve dimensions: identity stability, regulatory permission, mandate authority, inventory evidence, ownership transparency, conflicts and economics, information conduct, communication discipline, operational readiness, order quality, settlement performance and incident response.

Weights should reflect the business model. A firm sharing issuer-sensitive private-share inventory may weight information conduct and source lineage heavily. A transfer-intensive programme may weight operational readiness and settlement history. The adopted weights should be documented and stable enough to compare outcomes.

Each dimension needs observable evidence. A five-point scale might distinguish absent, weak, adequate, strong and independently evidenced performance. Descriptive anchors reduce score inflation. The reviewer records the source, evidence date, confidence and any limitation.

Scores should separate capability from behaviour. A counterparty may have sophisticated systems and poor communication discipline. Another may settle reliably while producing weak mandate evidence. The dimension view preserves these differences and supports targeted restrictions.

The total score can determine provisional tiers after gates pass. An approved counterparty may receive teasers; a qualified counterparty may receive controlled details; a transaction-approved counterparty may receive named live-block information; and a restricted counterparty may receive no further information. The actual tiers should follow applicable advice and internal policy.

Overrides should be rare, time-limited and visible. They should identify the exact dimension, reason, compensating control, approving person, permitted transaction and expiry. An override should not change the underlying evidence score.

Table 2. Twelve-dimension counterparty scorecard

Dimension	Illustrative weight	Strong evidence	Weak signal
identity stability	8%	independently verified entity and channels	inconsistent or changing identity
permission	12%	relevant current permission	scope unclear or restricted
mandate authority	10%	principal-confirmed current mandate	authority relayed through others
inventory evidence	10%	holder, class and quantity evidenced	repeated or unverifiable supply
ownership transparency	8%	controllers and beneficiaries resolved	opaque or shifting control
conflicts and economics	8%	complete payer-recipient bridge	unexplained spread or relationship
information conduct	10%	permissions observed and logged	onward sharing or leakage
communication discipline	6%	accurate, timely and version-controlled	pressure, ambiguity or off-channel use
operational readiness	7%	KYC, documents and settlement route ready	repeated incomplete packages
order quality	7%	authorised, conditioned and fundable demand	speculative or duplicated indications
settlement performance	10%	timely delivery and cash reconciliation	failures, delays or quantity breaks
incident response	4%	prompt containment and closure	concealment, delay or recurrence

Weights and thresholds are illustrative management assumptions.

7. Map ownership, conflicts and complete economics

Counterparty diligence should follow economic interests. The record identifies owners, controllers, affiliates, employees, fund vehicles, warehousing entities, beneficial parties and material commercial relationships. It connects these parties to the issuer, seller, buyer and other intermediaries.

Capacity should be explicit. An intermediary may act for the seller, buyer, issuer, warehouse, SPV or its own account. It may receive an introduction fee, placement fee, advisory fee, principal spread, carried interest, management fee, financing return or rebate. Each role should have authority and disclosure analysis.

The complete-economics bridge records source price, investor price, fees, financing, FX, tax, reserves, legal and administration costs, rebates, contingent payments and recipient. It distinguishes projected, agreed, invoiced, paid and collected amounts.

Hidden related parties can distort network assessment. A broker presenting independent demand may control the buyer vehicle. A source intermediary may be funded by the warehouse. A representative may have a personal interest in the issuer. These relationships should be investigated and governed based on facts.

Conflicts can affect information and allocation. A counterparty paid by volume may push unsupported size. A warehouse facing maturity may prefer the fastest buyer. An intermediary representing both sides may influence price or access. The file should describe the conflict, affected decision, control, approval and outcome.

The framework does not decide transaction-specific disclosure obligations. Qualified advisers should determine what must be disclosed, consented to, prohibited, separated or independently reviewed.

8. Grade information permission before revealing a live block

Information access should progress through controlled tiers. A network directory can hold public entity information. A pre-clearance tier can provide a generic sector and transaction type. A confidentiality-cleared tier can provide additional opportunity facts. Named issuer, seller, shareholder, price, cap-table, management and data-room information require transaction-specific permission.

The access record should state who may receive each field, for which purpose, through which channel, until when, and whether onward sharing is permitted. Recipient organisations should identify the people who need access rather than relying on an unrestricted corporate domain.

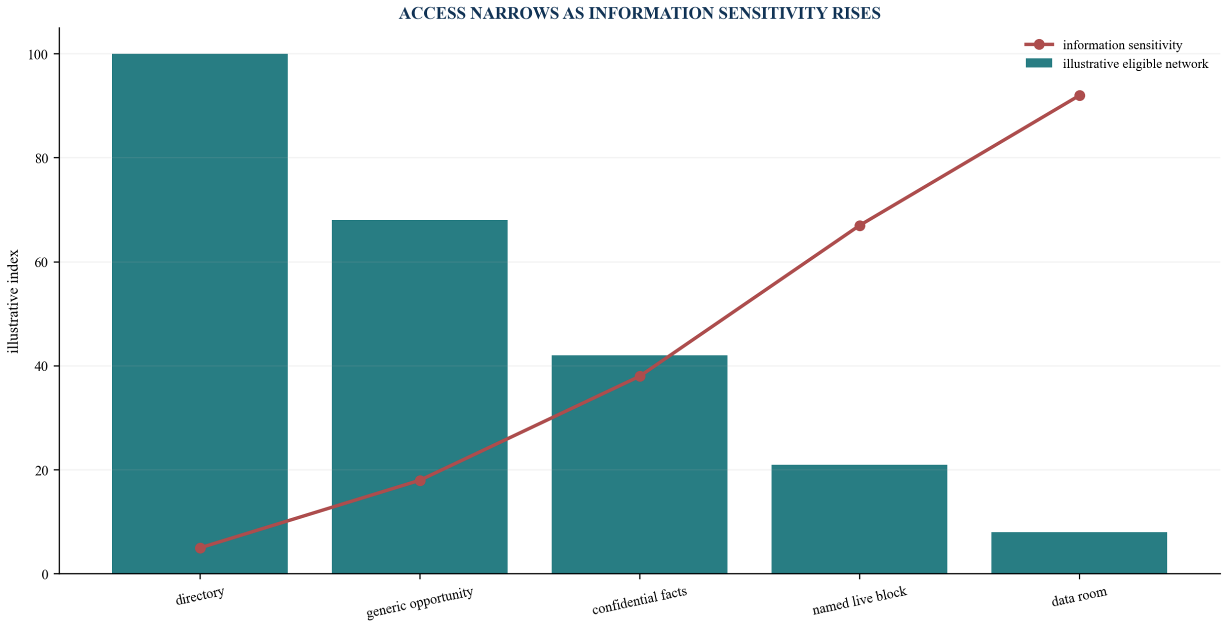
Teasers should be designed against re-identification. A combination of sector, geography, stage, revenue, ownership and timing may reveal an issuer even when its name is absent. The transaction owner should test whether the selected facts identify the opportunity to a market participant.

Watermarks, data-room access controls, expiry links and download restrictions can support governance. They do not replace permission decisions or recipient discipline. Sensitive communications should use approved channels with version history and revocation capability.

The network score should reflect actual conduct. Requests to use personal messaging, resistance to confidentiality, forwarding outside the approved team, or attempts to bypass the transaction owner are meaningful events. Positive conduct includes prompt recipient identification, accurate purpose statements and documented deletion or return.

Revocation should be operational. When a mandate ends, person leaves, incident occurs or transaction status changes, the system should withdraw access, notify relevant owners and preserve the evidence trail.

Figure 3. Progressive information-permission ladder



Information tiers are illustrative; transaction-specific confidentiality requirements control access.

9. Test communication conduct and claim quality

Communication conduct provides early evidence of counterparty quality. The review should assess accuracy, qualification of uncertainty, responsiveness, channel discipline, version control, pressure tactics, confidentiality and willingness to correct errors.

Claims should link to evidence. Statements about seller authority, buyer demand, price, allocation, issuer consent, transferability, timing or regulatory status need a source and an as-of date. The intermediary should distinguish confirmed facts from expectations and third-party representations.

Pressure can be diagnostic. Requests to share a name before confidentiality, accept a shortened diligence path, transfer funds to a newly supplied account, avoid counsel, conceal another intermediary or commit before documentation should trigger review. Urgency does not change evidence thresholds.

Version control matters when terms move quickly. Each circulation should identify the transaction, issuer where permitted, security, quantity, price, conditions, fees, expiry, source date and version. Corrections should be delivered to the same authorised population and preserved.

Communication quality should not become a personality score. The record uses observable events and defined anchors. Style, accent, geography, firm size or relationship seniority should not substitute for transaction evidence.

Positive evidence includes concise factual responses, disclosure of limitations, prompt correction, respect for access boundaries, accurate recipient lists and complete document delivery. Repeated patterns carry more weight than a single minor event.

Table 3. Communication-conduct evidence

Event	Evidence	Score effect	Control response
factual claim	source, date and qualification	positive when traceable	request support before reliance
term change	new version and recipient log	positive when controlled	withdraw obsolete version
urgency	reason and deadline	neutral when evidenced	keep standard gates active
off-channel request	message and requested action	negative where policy is bypassed	return to approved channel
correction	timing, scope and recipients	positive when complete	verify downstream update
confidentiality event	access and forwarding record	material negative if breached	contain, investigate and restrict

Assessments should use documented events and avoid unsupported character judgements.

10. Verify operational readiness before accepting claimed demand

An intermediary can produce persuasive market interest while lacking the operational ability to close. Readiness should cover investor identity, authority, eligibility, KYC and financial-crime checks, funding, documents, custodian, payment route, transfer restrictions, issuer process and timing.

Demand should progress through defined states: conversation, indication, conditional order, firm authorised order, funded order, allocated order and settled position. The counterparty should not receive outcome credit for an indication that never becomes an executable order.

Order evidence identifies the legal buyer, represented account, decision authority, security, quantity, price, conditions, expiry, funding status and transaction documents. Duplicate demand through several intermediaries should be resolved before the book is measured.

Operational readiness can be tested before sensitive details are shared. The intermediary can describe its standard investor verification, confidentiality, order, funding and settlement process. Where appropriate, prior transaction evidence may demonstrate capability without revealing client-confidential information.

Payment instructions need independent verification and change control. The system should compare beneficiary, bank, account, currency, reference and approved contract. A late change, personal account, unrelated beneficiary or unexplained jurisdiction should pause payment and trigger policy.

Readiness expires. KYC status, proof of funds, authority, mandate, tax forms or custodian instructions can become stale. The live transaction record should identify which evidence remains current for the contemplated close.

11. Control the moment a live block is shared

The sharing decision should be an auditable event. It identifies the counterparty entity and person, information tier, transaction, block quantity, permitted use, recipients, channel, expiry, restrictions, evidence state, score tier, gate results and approving owner.

A minimum record precedes release: verified identity and channel, relevant permission analysis, current representative authority, confidentiality, sanctions and financial-crime clearance, need-to-know purpose, and transaction-owner approval. Named inventory requires mandate and source-lineage evidence.

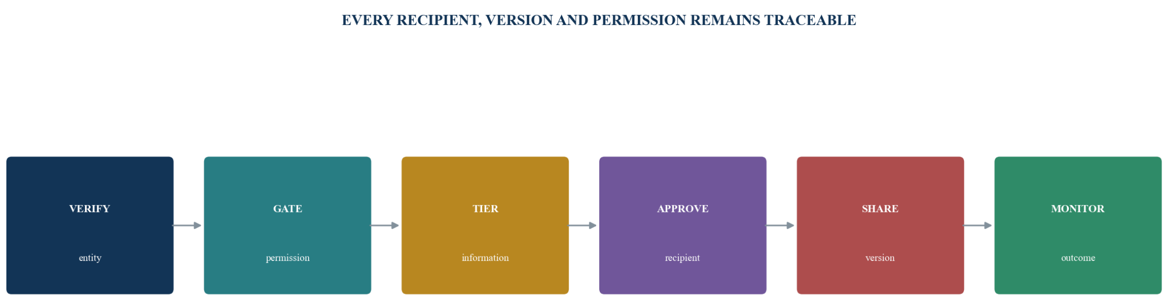
The block should carry a unique identifier and version. Quantity, class, price, conditions, fees, seller or issuer permissions, transfer route, evidence date and expiry appear according to the approved information tier. The recipient confirms limitations on onward distribution.

Parallel broker outreach should be controlled. Each recipient receives an allocation of information and, where relevant, market approach. Uncoordinated outreach can duplicate the block, reveal the holder, confuse price discovery or create conflicting representations.

The transaction owner should see who has received what. A dashboard shows current recipients, versions, access expiry, indications, orders, incidents and withdrawal instructions. This enables containment if inventory or authority changes.

Sharing outcomes feed the score. Accurate handling, qualified feedback, evidenced demand and compliance with restrictions improve the record. Leakage, misstatement, duplication or bypass attempts create events and may restrict future access.

Figure 4. Live-block sharing control sequence



The sequence is an author framework and requires adaptation to the transaction route.

12. Measure order and settlement outcomes

Historical outcomes provide evidence beyond reputation. The network ledger should connect opportunities, indications, authorised orders, funding, allocations, transfers, cash, failures, delays, complaints and final settlement.

Outcome measures should retain denominators. A counterparty that settles three of three allocated transactions differs from one that settles three of twenty. Volume, size, complexity, jurisdiction, security type and age help interpret the result.

Useful measures include evidence-to-order conversion, order-to-funding conversion, allocation acceptance, settlement completion, median settlement time, document completeness, quantity variance, price variance, failed settlement, withdrawal, reallocation, cash break and dispute incidence.

Cause codes prevent unfair attribution. An issuer refusal, seller withdrawal, rights process or platform outage may sit outside the intermediary's control. A missing buyer document, unsupported order, late funding or incorrect instruction may be attributable. Shared causes should be recorded as such.

Outcome quality also includes candour. A counterparty that identifies a problem early and supports remediation can be more reliable than one that conceals delay until closing. Incident response and recurring root causes should inform the forward tier.

The score should use a rolling window suited to transaction frequency. A small sample carries lower confidence. Recent performance and material incidents may deserve greater weight, subject to the approved methodology.

Table 4. Transaction-outcome ledger

Measure	Numerator	Denominator	Review question
evidence-to-order conversion	authorised orders	evidenced opportunities shared	does access produce executable demand?
funding conversion	funded orders	authorised orders	can represented buyers fund?
settlement completion	completed settlements	accepted allocations	do allocated trades close?
document readiness	complete first submissions	total submissions	how much rework is created?
timing quality	on-time settlements	completed settlements	are promised dates credible?
incident rate	attributable material incidents	active transactions	does risk recur?

Measures require complete populations and defined attribution rules.

13. Record incidents, complaints and adverse information fairly

The incident register should capture identity anomalies, permission concerns, mandate disputes, duplicated inventory, information leakage, misstatements, hidden fees, payment changes, failed settlement, complaints, litigation and regulatory or disciplinary information relevant to the relationship.

Official sources can support review. FINRA states that BrokerCheck reports can include registration history, qualifications, customer disputes, disciplinary events and certain criminal and financial matters. The FCA Register can include historical and restriction information. Public records require careful reading because pending allegations and final findings have different evidentiary status.

The record should distinguish report, allegation, pending matter, finding, sanction, remediation and closure. It identifies source, date, parties, relevance, response and reviewer. Unsupported rumours should not become factual adverse records.

Materiality should consider severity, recency, recurrence, connection to the proposed activity, client harm, candour and remediation. A minor historic administrative issue differs from a current activity restriction or repeated settlement misrepresentation.

Counterparty response should be preserved where appropriate. The reviewer tests the response against independent evidence and records remaining limitations. Commercial teams should not adjudicate reserved legal or regulatory questions.

Incident closure needs evidence. Containment, correction, reconciliation, notification, policy change, system control, training and effectiveness testing may be relevant. A closed incident remains in the historical record under the retention policy.

14. Make evidence expire and monitoring event-driven

Counterparty approval should have a defined validity period. Identity, permission, authority, ownership, sanctions, financial condition, mandate, contact channels, insurance, policies and transaction evidence can change at different speeds.

The evidence matrix assigns each item an owner, source, review frequency, expiry and event triggers. A regulatory permission may be checked before every material transaction. A corporate ownership record may follow periodic and event-driven review. A mandate expires on its own stated date or transaction change.

Triggers include personnel departure, domain change, payment change, ownership change, new affiliate, regulatory notice, complaint, sanctions alert, failed settlement, confidentiality event, unexplained price change, duplicate inventory or material change in transaction volume.

Monitoring should collect decision-relevant signals without creating uncontrolled surveillance. Data sources, lawful basis, access and retention require appropriate privacy and employment review. The network record should use professional evidence and avoid irrelevant personal information.

An expired item can downgrade or pause access automatically. The system identifies affected transactions and information permissions. Reapproval restores only the confirmed scope and records the new evidence.

Periodic reviews should sample the underlying proof rather than accept a green dashboard. The reviewer tests register extracts, firm confirmations, mandates, access logs, orders, settlements and incident closures.

15. Govern exceptions without corrupting the score

Transactions sometimes require judgement under incomplete conditions. The exception process should identify the precise missing evidence, reason for proceeding, affected decision, risk, compensating control, approver, duration and closure requirement.

The underlying score remains unchanged. An exception authorises a narrow action; it does not transform weak evidence into strong evidence. Dashboards should show both the calculated tier and any temporary permitted scope.

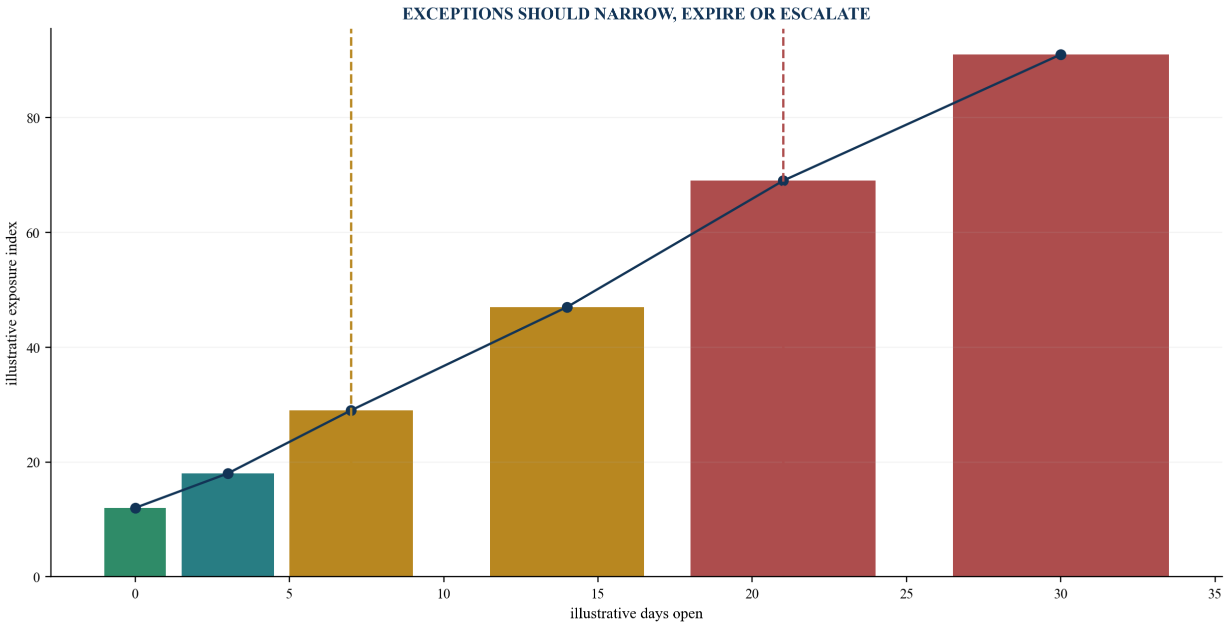
Stop-gate exceptions require especially careful treatment. Some failures may be non-waivable under law or policy. Qualified advisers and the designated control owner should determine whether any route exists. The relationship owner should not approve an exception to that person's own counterparty.

Compensating controls might include withholding named information, using an authorised principal, direct principal confirmation, reducing quantity, independent verification, separate escrow, additional approval, shorter expiry or supervised communication. The control should address the actual gap.

Expiry should be automatic. Continued access requires fresh evidence and a new decision. Repeated exceptions around the same counterparty or dimension signal a structural weakness and should affect governance review.

The governing body should see exception volume, age, concentration, reasons, approvers, transactions and outcomes. It should challenge whether commercial urgency is repeatedly displacing the adopted standard.

Figure 5. Exception ageing and escalation



Days and escalation bands are illustrative management assumptions.

16. Manage the network as a portfolio

Portfolio analysis reveals concentration and contagion. The dashboard should show exposure by intermediary entity, person, principal, group, issuer, security, geography, transaction type, information tier and relationship owner.

A large network can still depend on a few routes. Several branded intermediaries may share a common principal, beneficial owner, source holder or buyer population. The entity graph should identify these connections before management counts diversification.

The portfolio should distinguish approved contacts from active producing counterparties. Measures include opportunities shared, qualified orders, settlements, gross transaction value, information incidents, failed trades, open exceptions and age of evidence. Revenue should remain separate from transaction value.

Network coverage can be compared with mandate needs. A live seller mandate may require institutional buyers in a specific jurisdiction, while the network contains mostly introducers without relevant permission or execution capacity. The gap should be expressed as a capability need rather than a contact-count target.

Concentration limits can cover information exposure, live blocks, unsettled quantity, cash, issuer, source, intermediary group and relationship owner. Breaches prompt review and do not automatically imply wrongdoing.

The portfolio dashboard should support commercial decisions. It can identify counterparties deserving deeper engagement, routes requiring remediation, and areas where a new mandate cannot be executed within the approved network.

Table 5. Network portfolio dashboard

View	Measure	Decision	Risk signal
permission	active entities by relevant scope	usable execution capacity	expired or mismatched scope
information	recipients by access tier	controlled market reach	concentrated named access
opportunity	evidenced blocks and mandates	qualified transaction pipeline	duplicate or stale inventory
demand	authorised and funded orders	executable buyer coverage	speculative indications
settlement	completion, time and breaks	reliable counterparties	recurring attributable failures
economics	contracted, invoiced and collected fees	realised commercial outcome	forecast reported as collection

Targets and limits should be formally adopted for the firm's business model.

17. Build the data architecture around immutable events

The data model should connect entity, person, principal, permission, mandate, inventory lot, transaction, information grant, communication, order, allocation, payment, settlement, incident, evidence item, score and exception.

Every material change creates an event with timestamp, actor, source, prior state, new state and approval. A person moving firms does not overwrite prior affiliation. A changed mandate does not erase the original. A revised score retains its previous evidence and methodology.

Permissions should travel with data. The system knows which user can see the seller, issuer, broker, investor, price, order, complaint and adverse record. Exports should inherit restrictions and be logged.

Automated rules can flag expiry, domain mismatches, duplicated inventory, hidden relationships, unexplained term changes, orders without authority, settlement breaks and exception age. Material decisions remain under named human authority, with the rule version and override visible.

The network tool should integrate with transaction and CRM systems while preserving different evidence classes. A CRM interaction shows relationship activity. It should not be treated as verified permission, mandate or settlement evidence unless the required documentation is linked.

Data quality controls include mandatory identifiers, valid states, source dates, duplicate detection, reconciliations, restricted fields and review queues. Access, retention, correction and deletion follow applicable law, contracts and investigation holds.

18. Run a ten-day broker-network quality diagnostic

Days one and two define the network population, entities, people, principals, services, jurisdictions, transaction types, live blocks and information stores. The team identifies the economic buyer and the decisions at risk.

Days three and four sample identity, regulatory status, permissions, representative authority, contacts, ownership, sanctions screening and confidentiality. Critical gate failures receive immediate containment owners.

Days five and six sample mandates, inventory, source lineage, communications, economics, orders and payment instructions. The review compares claims with evidence and identifies duplicated or expired blocks.

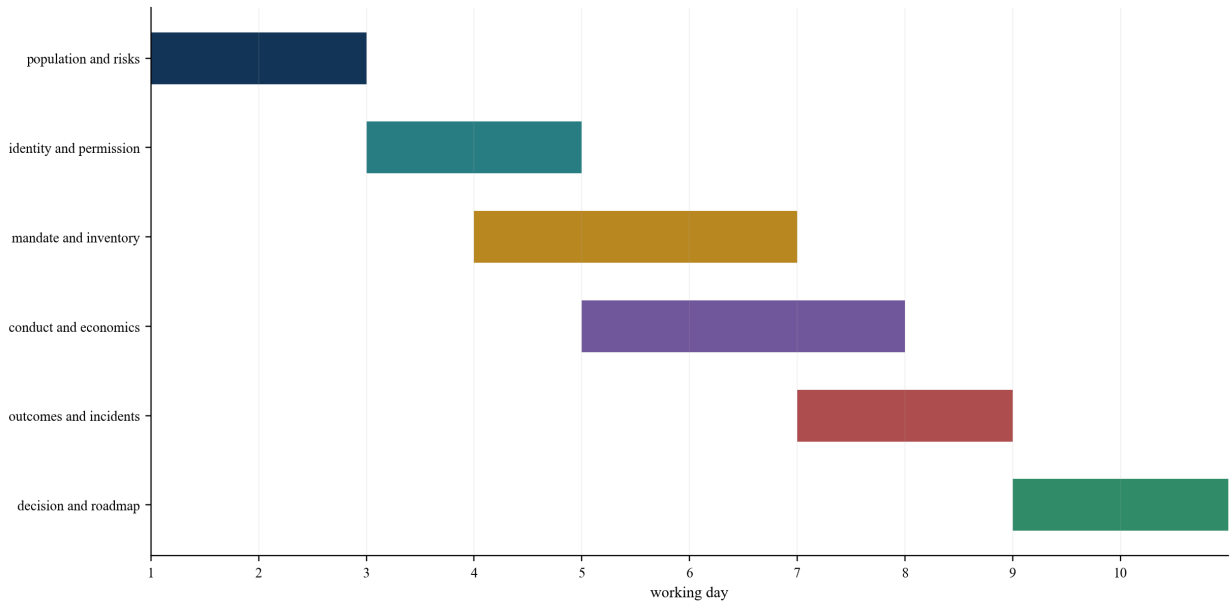
Days seven and eight reconstruct settlement outcomes, failures, complaints, incidents, exceptions and access history. The team builds an entity graph and tests whether apparent network breadth represents distinct capacity.

Day nine scores maturity across gates, evidence, information, conduct, operations, outcomes, monitoring, data and governance. Scores remain separate from verified stop failures.

Day ten presents a decision-ready remediation plan, qualified counterparty population, restricted list, urgent transaction controls, target operating model, delivery assumptions, owners and thirty-day implementation roadmap.

Figure 6. Ten-day diagnostic workplan

FROM NETWORK POPULATION TO CONTROLLED LIVE-BLOCK ACCESS



Timing is an illustrative delivery assumption subject to data access and scope.

19. Implement a thirty-day counterparty control office

Days one to five establish governance, scope, entity and person identifiers, capacity taxonomy, stop gates, evidence standards, decision rights and incident escalation.

Days six to ten reconcile the active network against official registers, firm confirmations, ownership records, sanctions screening and contact-channel evidence. The team assigns evidence owners and expiry.

Days eleven to fifteen implement mandate, inventory, source-lineage, economics and information-permission records. Live blocks receive current identifiers, versions and controlled recipient lists.

Days sixteen to twenty configure the twelve-dimension scorecard, descriptive anchors, tier rules, exception workflow and counterparty review pack. Historical cases test the methodology.

Days twenty-one to twenty-five load orders, settlements, incidents and outcomes. The team resolves duplicates, assigns cause codes and establishes confidence measures for small samples.

Days twenty-six to thirty train users, test access revocation and incident response, close critical findings, establish periodic assurance and obtain management acceptance. Unresolved issues retain named owners and deadlines.

Table 6. Thirty-day control-office deliverables

Workstream	Deliverable	Acceptance evidence	Owner
identity	entity, person and principal master	sampled independent verification	network control owner
permission	activity and jurisdiction map	current source evidence	compliance owner
authority	mandate and inventory ledger	principal and source lineage tested	transaction owner
information	tier and recipient control	access and revocation test	information owner
score	gates, dimensions and exceptions	historical cases reproduced	independent reviewer
outcomes	order, settlement and incident dashboard	reconciled transaction sample	management owner

Scope should reflect network size, transaction volume, systems and applicable regulation.

20. Package the work around urgent paid outcomes

The framework can support a broker-network diagnostic, counterparty remediation, live-block sharing protocol, mandate and inventory control build, intermediary scorecard, official-register verification programme, settlement-performance review, information-leakage response or recurring network control office.

Commercial qualification should identify the active consequence: a block ready for circulation, duplicated supply, uncertain broker authority, information leakage, repeated failed settlement, a new geography, a regulator or auditor finding, a board deadline, or a mandate whose buyer network cannot yet be evidenced. The economic buyer should own the decision, data and budget.

The engagement should define entities, people, jurisdictions, activities, securities, live transactions, systems, evidence, decisions, deliverables, advisers, exclusions and reliance limitations. Reserved legal, regulatory, brokerage, sanctions, valuation, accounting, audit and tax functions remain with appropriately qualified and authorised providers.

Fees can reflect network size, entity and person complexity, jurisdictions, live-block urgency, historical reconstruction, register verification, data remediation, system integration and ongoing monitoring. Any transaction-linked component requires current legal and regulatory review and an executed agreement.

Commercial reporting should distinguish opportunity, proposal, mandate, invoice, collection and contribution after delivery cost. Evidence of a collected fee requires an executed mandate, valid invoice and cleared bank receipt. Pipeline and forecasts remain management estimates.

The strongest offer connects a costly transaction problem to a defined outcome: a verified counterparty population, controlled information access, credible inventory, fewer avoidable settlement failures, an auditable decision record and a network that can support live mandates.

References

[1] US Securities and Exchange Commission. Broker-Dealers: Capital Raising Building Blocks. https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/broker-dealers

[2] US Securities and Exchange Commission. What is a Broker-Dealer? July 2026. https://www.sec.gov/files/oasb-broker-dealer-building-block.pdf

[3] Financial Industry Regulatory Authority. About BrokerCheck. https://www.finra.org/investors/investing/working-with-investment-professional/about-brokercheck

[4] Financial Industry Regulatory Authority. Rule 2090: Know Your Customer. https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090

[5] Financial Industry Regulatory Authority. Rule 3110: Supervision. https://www.finra.org/finramanual/rules/r3110/

[6] Financial Industry Regulatory Authority. Private Placements: Regulatory Obligations and Related Considerations. https://www.finra.org/rules-guidance/guidance/reports/2024-finra-annual-regulatory-oversight-report/private-placements

[7] Financial Conduct Authority. Financial Services Register. Updated 13 February 2026. https://www.fca.org.uk/firms/financial-services-register

[8] Financial Conduct Authority. How to Check a Firm or Individual is Authorised. Updated 3 September 2025. https://www.fca.org.uk/consumers/how-check-firm-individual-authorised

[9] Financial Conduct Authority. Clone Firms and Individuals. Updated 14 May 2025. https://www.fca.org.uk/consumers/clone-firms-individuals

[10] Dubai Financial Services Authority. Public Register: Firms. https://www.dfsa.ae/public-register/firms

[11] Dubai Financial Services Authority. DFSA Cautions: DFSA's Public Register Cloned. 11 February 2025. https://www.dfsa.ae/alerts/dfsa-cautions-dfsas-public-register-cloned

[12] Abu Dhabi Global Market. Official Public Registers. https://www.adgm.com/public-registers/

About the Author

Chennakeshav Adya, Independent Researcher