Surveillance for Private Markets: Detecting Duplicate Inventory and Impossible Access

A Global Evidence, Alert and Case-Management Framework for Private-Share Transactions

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

Private-market activity produces surveillance problems without a central order book. The same share block can circulate through several brokers, quantities can exceed the holder's evidenced position, access can be claimed through incompatible routes, and counterparties can receive sensitive information despite expired permissions. Quotes, orders, allocations and settlements often live in separate systems. Commercial urgency can turn weak signals into apparent market depth before anyone reconstructs the underlying ownership, mandate and information chain.

This paper develops a global evidence, alert and case-management framework for private-share surveillance. It fingerprints inventory at holder, security, quantity, mandate and rights levels; builds a source-lineage graph; tests whether claimed access is feasible; records every quote, order, communication, permission and settlement as an immutable event; detects duplicate supply, recycled demand, impossible capacity, price and quantity anomalies, unauthorised information access, suspicious sequencing and settlement divergence; routes alerts by severity and confidence; preserves case evidence; and feeds outcomes back into counterparty controls. The framework includes a private-market risk assessment, alert library, evidence-confidence model, network graph, quantity reconciliation, information-access heat map, ten-day diagnostic and 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. Public-market surveillance and reporting requirements do not automatically apply to every private transaction. Applicable duties depend on the firm, activity, security, client, market, jurisdiction, capacity, communication and route. Current legal, regulatory, compliance, sanctions, data-protection, tax and accounting advice is required. Worked values, thresholds, weights, timelines and scenarios are management assumptions used solely to demonstrate the framework.

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

Keywords: private-market surveillance, duplicate inventory, impossible access, private shares, source lineage, information controls, anomaly detection, settlement risk

1. Start with the risks unique to private-market surveillance

Private-market surveillance should protect decisions around inventory, access, information, price, demand, allocation and settlement. It should reveal patterns that individual relationship owners cannot see from their own conversations.

The surveillance population includes opportunities, issuers, securities, holders, mandates, inventory lots, intermediaries, recipients, quotes, indications, orders, allocations, vehicles, payments, transfers and incidents. An event can be suspicious or unreliable without constituting market abuse. The operating framework should preserve this distinction and route any reserved regulatory judgement to qualified advisers.

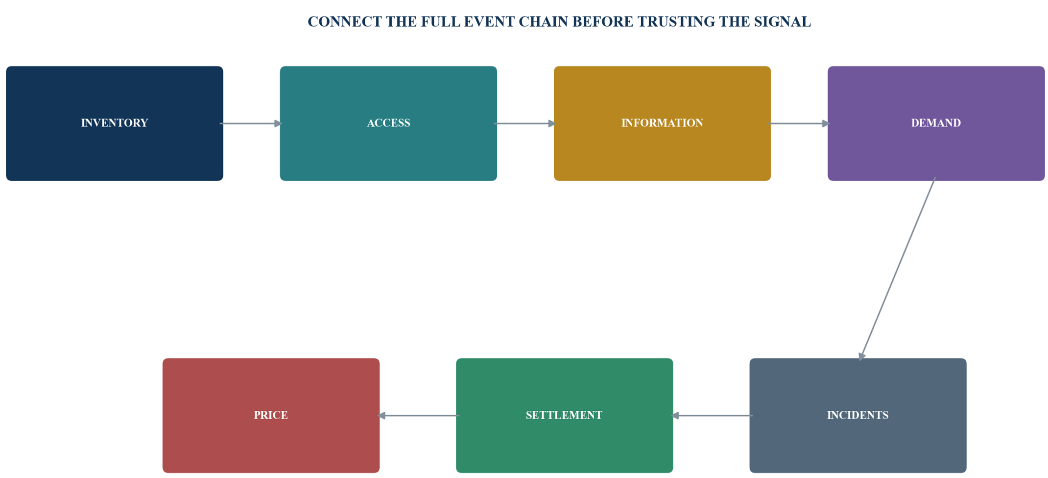
The first risk is false depth. One holder's block can appear through several brokers, each presenting the full quantity. A second risk is impossible access: an intermediary claims authority from an issuer, seller, platform, fund or employee that cannot support the represented route. A third risk is informational: the opportunity travels beyond approved recipients or survives after permission expires.

Additional risks include recycled buyer demand, coordinated or circular indications, inconsistent rights descriptions, price signalling unsupported by executable interest, orders that disappear when evidence is requested, payment instruction changes, allocations exceeding controlled inventory and settlement results that contradict the marketed state.

The framework requires a business-specific risk assessment. It maps how the organisation could facilitate misstatement, leakage, duplication, manipulation, fraud, unauthorised activity or failed settlement. The FCA's Market Watch 69 emphasises surveillance arrangements proportionate to business scale and nature, comprehensive coverage of orders and trades, review of alert logic, and effective investigation of alerts.

The surveillance objective is actionable evidence. Alerts should identify a transaction decision, affected parties, source records, confidence, severity and required response. A large alert count without prioritisation can conceal material cases.

Figure 1. Private-market surveillance risk map



Regulatory characterisation requires transaction-specific advice.

2. Define a canonical security and holder record

Duplicate detection begins with a stable security identity. The record should distinguish issuer, legal entity, security class, series, currency, nominal or par value, rights, seniority, conversion, voting, transfer restrictions, legends, custodian or administrator and governing documents.

Names alone are unreliable. The same class may be described as ordinary, common, common stock, employee common, secondary common or a platform-specific label. A surveillance system should map aliases to the canonical security while preserving the original language and source.

The holder record identifies registered holder, beneficial holder, nominee, custodian, fund, vehicle, controller, relationship to the issuer, evidence source and as-of date. A holder's legal and beneficial positions can differ. Transferable quantity may be lower than gross ownership because of pledges, options, commitments, restrictions or prior allocations.

The US Securities and Exchange Commission notes that private-company securities are often illiquid and may be restricted. Resale routes can have conditions concerning holder status, holding periods, purchasers, manner of sale and information. Surveillance should preserve the claimed route and the evidence supporting it without assuming transferability.

Corporate actions require versioning. Splits, conversions, tenders, repurchases, option exercises, reorganisations and financings can change quantity and rights. The system should reconcile the security master before comparing supply across time.

The position record should expose confidence. Direct issuer or transfer-agent evidence may carry higher confidence than an intermediary representation, subject to authenticity and authority. The methodology should document its evidence hierarchy and limitations.

Table 1. Canonical inventory record

Field group	Core fields	Preferred evidence	Surveillance use
issuer	legal entity, jurisdiction and identifiers	official and issuer records	resolve names and entities
security	class, series, rights and restrictions	governing and cap-table records	compare like with like
holder	registered, beneficial and controlled parties	issuer, transfer-agent or custodian evidence	identify unique origin
quantity	gross, encumbered, committed and available	dated position evidence	calculate deliverable supply
route	exemption, consent and transfer process	current specialist analysis	test feasibility
evidence	source, date, reviewer and confidence	preserved source artefact	support alert decisions

Evidence hierarchy and validity periods require formal adoption.

3. Fingerprint each inventory lot before adding market depth

An inventory fingerprint combines issuer, security class, beneficial holder, registered holder, source lineage, quantity band, price band, mandate date, restrictions, contact, settlement route and document hashes. It helps identify records that may represent the same underlying block.

Exact matching catches identical identifiers, documents or quantities. Fuzzy matching catches similar issuer names, rounded quantities, slightly changed prices, relayed contacts and common narrative errors. Network matching identifies several brokers connected to one source holder or mandate.

The fingerprint should not create an unsupported conclusion. Two records with similar quantities may be legitimate separate positions. An alert marks a question and preserves the compared evidence. Confirmation requires source or principal verification.

Quantity splitting deserves special treatment. A holder may authorise several intermediaries for different slices, or one intermediary may present smaller tickets from one larger block. The system should record whether quantities are exclusive, overlapping, aggregate-limited or independently controlled.

Document hashes can reveal reused evidence. The same cap-table extract, statement, screenshot or mandate circulated under different descriptions should trigger review. Visual or metadata changes can require additional comparison when files are re-exported.

Fingerprints expire when a material attribute changes. A new price alone may create a revised event. A new holder, security, mandate, route or quantity creates a new inventory state linked to the prior one.

4. Build a source-lineage graph rather than a flat broker list

Source lineage traces the opportunity from holder or issuer through every intermediary to each recipient. Each edge states who introduced whom, what authority was represented, what information was shared, the transaction role, economic interest, evidence and dates.

A graph exposes convergence. Several brokers may lead back to the same holder, employee, adviser, platform or vehicle. It also exposes divergence when one source produces inconsistent price, quantity, rights or seller identity through different routes.

The graph should distinguish verified and represented edges. A direct firm confirmation can verify that a person acts for the firm. A broker's statement that another broker controls the seller remains represented until independently confirmed.

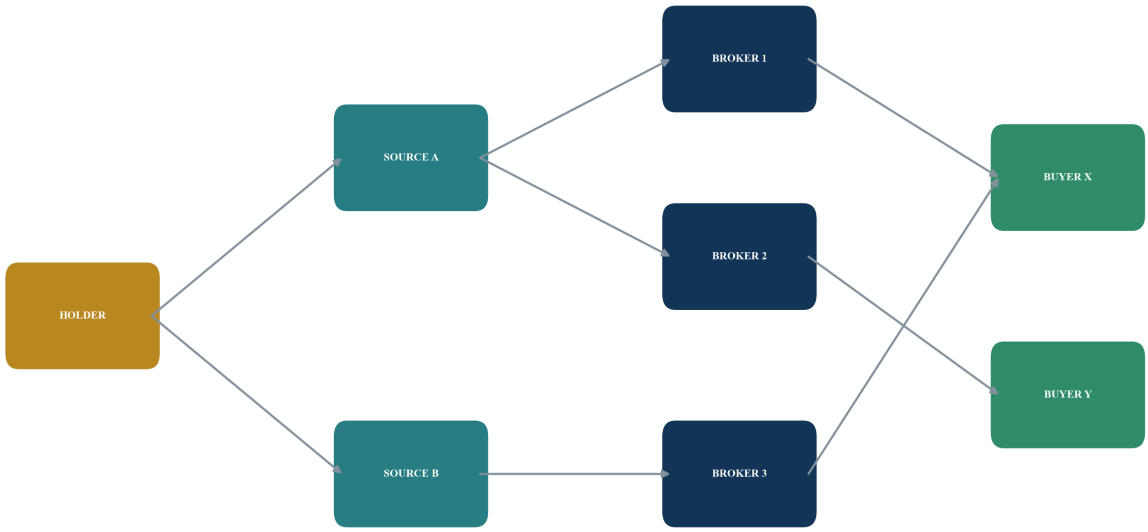
Ownership and compensation edges matter. A source intermediary may control a buyer vehicle, share fees with another party or fund a warehouse. These relationships can explain repeated demand, coordinated quotes or pressure to circulate information.

The access path should end at a permissible transaction route. A chain of introductions does not itself establish that every person can solicit, arrange, recommend, advise, hold money or settle the security. The earlier counterparty gate remains active.

Graph analytics should support review, not produce guilt by association. A shared source can be legitimate. The system should show the evidence and decision consequence without unsupported character judgements.

Figure 2. Source-lineage convergence graph

MULTIPLE ROUTES CAN REPRESENT ONE BLOCK OR ONE BUYER



Nodes and relationships are illustrative management assumptions.

5. Test whether claimed access is feasible

Impossible access means that a claimed route cannot support the represented transaction state. The test asks whether the intermediary, mandate, holder, security, information and settlement process can coexist as described.

Entity feasibility covers the legal existence, identity and current contact channel of every material party. Permission feasibility maps the actual activity and jurisdiction. Authority feasibility tests whether the person can act for the named principal within the mandate's scope and period.

Inventory feasibility tests whether the holder controls the security and quantity after commitments, restrictions and other allocations. Information feasibility tests whether the source may disclose the opportunity and whether the recipient may receive it. Settlement feasibility tests whether consents, transfer documents, money and ownership records can reach finality.

Contradiction rules can identify impossible combinations: an expired mandate with a current live quote; a broker claiming issuer approval when the issuer is unaware; a quantity greater than evidenced ownership; a restricted class described as freely transferable; a buyer order predating receipt of the permitted information; or settlement through a party absent from the transaction documents.

The alert should preserve the represented fact and conflicting evidence. It should not silently correct the record. The case owner determines whether the contradiction reflects stale data, a genuine change, misunderstanding, duplicate route or misconduct.

Material impossible-access alerts should pause further sharing, order acceptance, allocation, payment or completion statements according to policy. Qualified advisers determine any reporting or notification duty.

Table 2. Impossible-access tests

Test	Claimed state	Conflicting evidence	Initial response
identity	authorised firm contact	domain or telephone mismatch	quarantine channel
authority	representative controls source	principal does not confirm role	pause access
mandate	live exclusive block	mandate expired or held elsewhere	reverify inventory
quantity	full block deliverable	holder evidence below quantity	cap or pause supply
information	recipient cleared	confidentiality or purpose absent	revoke sharing
settlement	closing-ready route	required consent or account missing	stop completion claim

Rules are illustrative and require transaction-specific calibration.

6. Record quotes, orders and communications as immutable events

Surveillance needs history. A spreadsheet or CRM field that overwrites the latest price or quantity destroys the sequence that could reveal duplication, recycling or manipulation.

Each event carries transaction, issuer, security, inventory lot, party, person, capacity, timestamp, channel, state, quantity, price, conditions, evidence, prior event and permission. Attachments receive stable hashes and access metadata.

Quotes progress through represented, evidenced, approved for sharing, executable, withdrawn, expired and superseded states. Demand progresses through enquiry, indication, conditional order, authorised order, funded order, allocation and settlement. A cancelled or amended event remains in the record.

The FCA states that surveillance can need to cover orders as well as completed trades, including cancelled and amended orders. Private-market surveillance can apply the same operational lesson: non-settled events may contain meaningful patterns, even when a public-market reporting regime does not apply.

Communications should identify recipients and content version. A teaser, named block, data-room invitation, price update and allocation notice have different information sensitivity. The event model should support revocation and incident reconstruction.

Clock quality matters. Systems should use synchronised timestamps and preserve original message dates where imported. Late entry, backdating and timezone conversion should be visible to the reviewer.

7. Create an alert library tied to decision consequences

The alert library should begin with the risk assessment. Each scenario identifies the behaviour, data inputs, logic, lookback, threshold, exclusions, severity, confidence, owner, response and testing method.

Duplicate inventory alerts compare fingerprints, source lineages and aggregate holder quantities. Recycled demand alerts identify the same buyer or beneficial owner appearing through several intermediaries. Impossible-access alerts compare authority, mandate, permission and route.

Information alerts detect new recipients, forwarding, access after expiry, personal-channel use, downloads outside the approved population and inconsistent teaser versions. Price alerts identify rapid unexplained changes, crossed indications, circular reference points and large deviations among comparable observations.

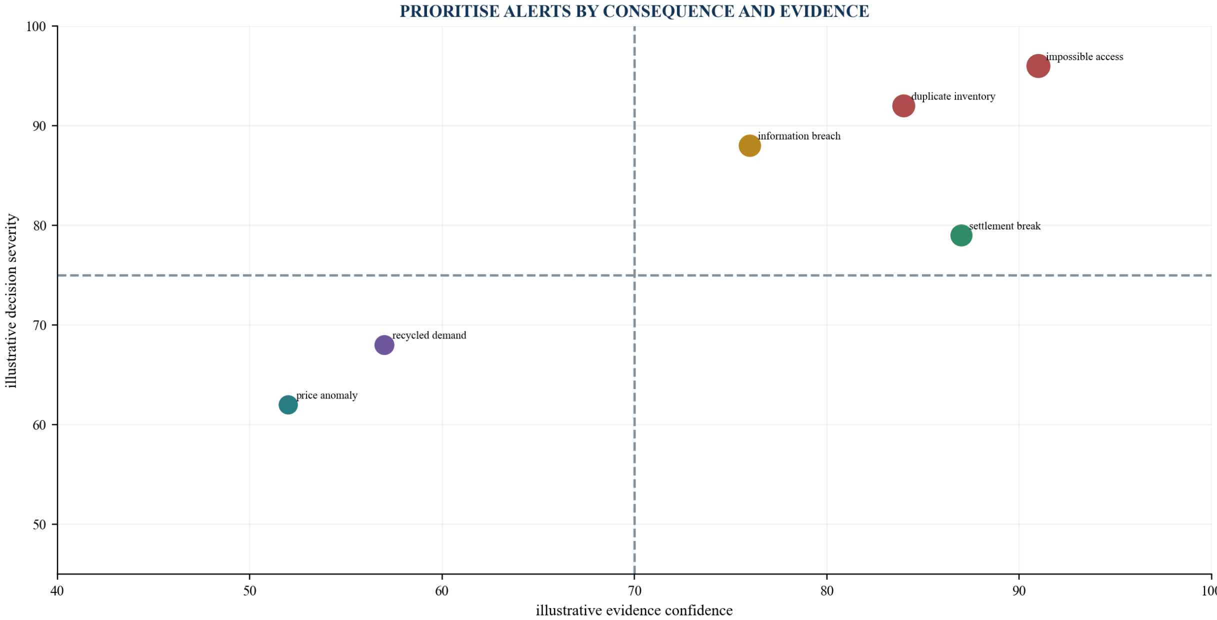
Quantity alerts identify supply or allocations above controlled inventory, repeated round amounts and sudden expansion after scarcity is communicated. Sequencing alerts identify orders preceding access, allocations preceding approval, funding preceding documents, or completion claims preceding registration.

Settlement alerts identify mismatched beneficiary, cash shortfall, late funds, quantity breaks, missing consent, failed registration, unexplained reallocation and repeated incidents attributable to the same route.

Every alert should point to an action. The immediate consequence might be review, restriction, independent confirmation, access revocation, payment verification, reconciliation or case escalation. Alerts without a decision owner create noise.

Figure 3. Illustrative surveillance alert library

PRIORITISE ALERTS BY CONSEQUENCE AND EVIDENCE



Scores and thresholds are illustrative management assumptions.

8. Detect duplicate inventory without overstating certainty

Duplicate detection should combine deterministic and probabilistic tests. Exact document hashes, mandate identifiers, holder identifiers or inventory-lot IDs can provide strong signals. Similar quantity, price and wording can provide weaker signals requiring review.

The comparison should occur at several levels. Lot-level duplication asks whether two records represent the same controlled block. Holder-level overstatement asks whether aggregate active supply exceeds the holder's evidenced available position. Market-level inflation asks whether the same block appears through several routes and is being counted as independent depth.

Time windows should reflect transaction behaviour. A block withdrawn yesterday and reintroduced today may be a valid revised mandate. A record that remains active after the mandate expires is stale. The engine should preserve both cases and apply appropriate status logic.

Allocation commitments reduce availability. Once quantity is reserved, signed, funded or transferred, it should move through defined states. The surveillance engine compares the remaining amount with new claims.

Thresholds should account for rounding and partial slices. A broker may quote approximately ten million shares when the evidenced amount is 9.8 million. The review should decide whether the difference is presentation, change or contradiction.

Confirmed duplicates should update the market view without deleting history. The system links the routes to one unique origin, recalculates controlled supply and records who received corrected information.

9. Detect recycled and impossible demand

Buyer demand can be duplicated through advisers, brokers, fund vehicles and related entities. The buyer master should connect legal entity, beneficial owner, represented account, decision maker, fund, adviser and source intermediary.

Order fingerprints use security, buyer, beneficial owner, quantity, price, conditions, timing, funding and narrative. Similar orders entering through several routes should trigger identity and authority review before they are added to demand.

Impossible demand includes an investor whose mandate excludes the security, an order larger than available or authorised capacity, a commitment predating internal approval, a fund outside its investment period, an account without KYC, or a buyer that cannot use the proposed transfer route.

Demand should retain evidence states. A conversation is not an indication. An indication is not a firm order. A signed order subject to conditions is not funded demand. Surveillance compares actual state with the language used in management and market communications.

Circular demand can arise when the seller, warehouse, affiliate or intermediary controls a buyer vehicle presented as independent interest. Ownership and related-party graphs should inform alert review.

The system should protect legitimate confidentiality. Resolution can use a restricted beneficial-owner function, hashed identifiers or an independent reviewer where the full identity should not be visible to the commercial team.

Table 3. Demand-surveillance states

State	Minimum evidence	Permitted description	Alert trigger
enquiry	identified recipient and question	enquiry	reported as demand
indication	entity, quantity, price and conditions	non-binding indication	duplicated beneficial owner
authorised order	authority and complete terms	order subject to stated conditions	authority absent
funded order	cleared funds under approved route	funded order	beneficiary or amount mismatch
allocation	approved quantity and terms	allocated interest	exceeds controlled inventory
settlement	cash and ownership finality evidence	settled position	ledger divergence

State definitions should align with governing documents and applicable duties.

10. Monitor information access as carefully as orders

Private-market information can create value and harm before a transaction occurs. Surveillance should connect each recipient to the transaction, information tier, purpose, confidentiality record, permitted fields, channel, version, grant time, expiry and revocation.

Impossible information access includes a person receiving named issuer data before confidentiality, an entity outside the approved jurisdiction, a former employee retaining data-room access, an intermediary forwarding materials to an undisclosed buyer, or a recipient accessing a version beyond the transaction purpose.

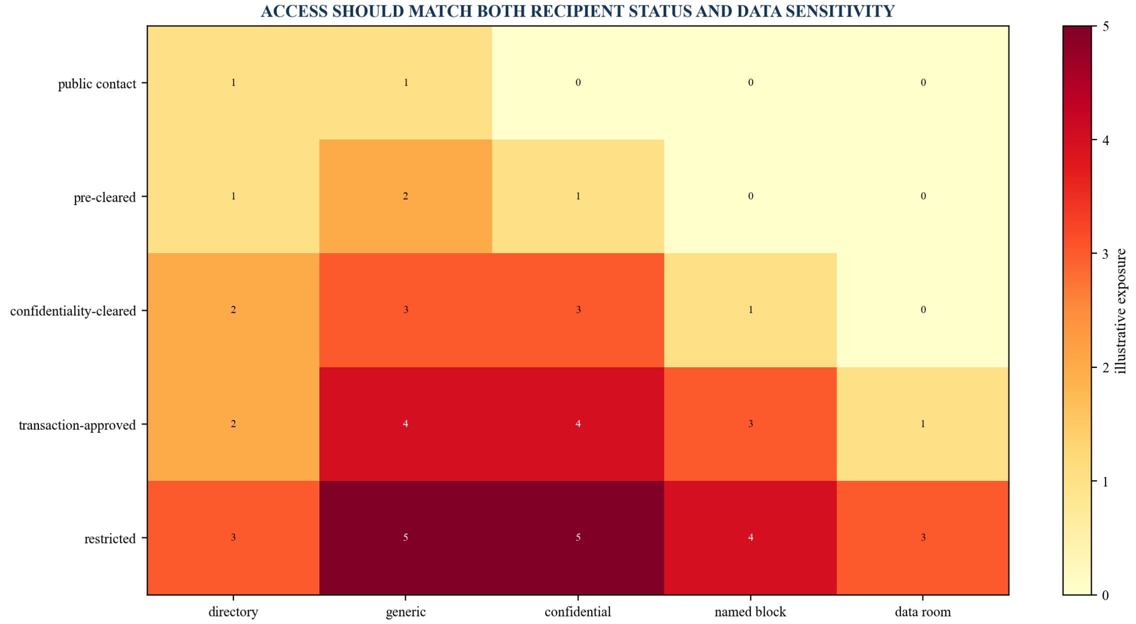
Access analytics can identify unusual download volume, off-hours activity, new geographies, repeated failed authentication, mass forwarding, personal email use and access after a mandate ends. These are signals requiring context, not automatic findings.

The system should test teaser re-identification. A nominally anonymous teaser can identify an issuer through the combination of sector, location, revenue, funding stage, customers and timing. The transaction owner should approve the fact set.

Watermarks and data-room logs support cases. They should be protected, retained and interpreted according to applicable privacy, confidentiality and employment requirements. Monitoring scope should be proportionate and disclosed where required.

An incident should trigger containment: suspend the affected access, preserve evidence, identify recipients, determine which information travelled, assess transaction consequences and obtain specialist advice on notification or reporting.

Figure 4. Information-access exposure heat map



Values are illustrative management assumptions.

11. Compare price and quantity in a rights-aware market view

Price surveillance requires comparability. A preferred share, common share, option, forward interest and SPV interest can have different rights, fees, timing and transfer conditions. A raw price comparison can create false alerts.

Each observation should retain security rights, quantity, state, source, unique origin, timestamp, conditions, fees, FX, settlement route and permitted use. Adjustments and exclusions should be documented.

Alerts can identify rapid changes unsupported by new information, opposite quotes from the same origin, large deviations from comparable evidence, price improvement paired with weaker settlement conditions, and repeated reference to a transaction that cannot be evidenced.

Quantity surveillance compares holder position, active mandates, marketed supply, orders, allocations and settlements. It shows the conservation equation: evidenced available inventory equals unallocated controlled quantity plus allocated unsettled quantity plus settled or otherwise disposed quantity, subject to explained changes.

Sparse evidence requires caution. A wide price range or small number of observations should be reported with confidence and limitations. The system should avoid converting private-market noise into a precise public-style market price.

Price and quantity alerts should reopen the transaction decision when they affect fairness, economics, information, inventory control or settlement feasibility.

12. Use settlement outcomes to validate earlier signals

Settlement provides a powerful feedback loop. It tests whether represented inventory, authority, demand and process reached cash and ownership finality.

The closing record links agreement, seller, buyer, security, quantity, price, fees, bank receipt, escrow or safeguarding record, issuer or transfer-agent registration, vehicle ledger and accounting record. Differences remain open exceptions.

An inventory route that repeatedly fails on title, consent or quantity may have shown early duplicate or impossible-access signals. A buyer route that repeatedly withdraws, misses funding or cannot complete documents may have shown recycled or impossible-demand signals.

The model should compare alert outcomes with settlement causes. Confirmed alerts, false positives, missed issues and unresolved cases inform rule tuning. A low alert rate can indicate clean activity or inadequate coverage; testing must distinguish them.

Outcome attribution should be evidence-led. Issuer refusal, seller withdrawal, legal change, platform outage and counterparty failure have different causes. Shared and unknown causes should remain visible.

Surveillance should continue through post-close reconciliation. Reversals, refunds, delayed registration, amended ledgers and complaints can change the final outcome.

Table 4. Alert-to-outcome feedback

Alert family	Pre-close signal	Closing evidence	Model response
duplicate inventory	convergent sources or excess quantity	actual deliverable lot	refine fingerprint logic
impossible access	authority or route contradiction	consent and registration result	update feasibility rules
recycled demand	common buyer or account	funding and beneficial owner	strengthen identity graph
information	unauthorised or expired access	incident and recipient record	revise permissions and alerts
price	unexplained non-comparable deviation	final terms and complete economics	improve comparability bridge
settlement	readiness or payment mismatch	cash and ownership finality	update counterparty score

Outcomes require documented attribution and complete populations.

13. Triage alerts by severity, confidence and immediacy

Alert queues should prioritise decision consequences. Severity reflects potential investor, issuer, seller, firm, regulatory, financial and reputational impact. Confidence reflects evidence quality, rule precision and corroboration. Immediacy reflects the next irreversible act.

A high-severity, high-confidence alert before information release, allocation, payment or completion requires prompt action. A lower-confidence alert can still justify a limited pause when the next act is irreversible.

The triage record identifies transaction, alert scenario, affected parties, evidence, conflicts, open decisions, current exposure, owner, deadline and immediate control. Automated severity should be reviewable.

The reviewer should avoid closing an alert solely because no obvious link exists between the parties. FCA Market Watch 69 reports weaknesses where firms closed surveillance exceptions based on the absence of an obvious client-to-issuer link. Private-market networks can contain indirect relationships that require graph analysis.

False positives should be recorded with reasons. A valid repeated holder mandate, authorised slice, common platform route or legitimate related vehicle may explain the signal. The resolution becomes a test case for future calibration.

Backlogs require governance. Age, severity, transaction stage, owner and open exposure should be visible. A stale alert tied to a settled transaction still needs closure and potential historical remediation.

14. Investigate cases with independence and evidence discipline

A case begins when an alert requires structured review. The case file preserves the original alert, data inputs, rule version, source documents, communications, access logs, orders, payments, interviews, decisions and remediation.

The investigator should be independent from the commercial decision under review. Conflicts, prior involvement and reporting lines should be recorded. Legal privilege and investigation confidentiality require specialist advice.

The case distinguishes facts, representations, hypotheses, findings and unresolved questions. It records contradictory evidence and the basis for conclusions. Unsupported allegations do not become factual counterparty labels.

Containment can include suspending access, freezing allocation, verifying payment instructions, contacting the principal through an independent channel, correcting recipients, preserving data or escalating to legal and compliance. The response should be proportionate to the evidence and next act.

Qualified advisers determine whether a matter triggers regulatory, suspicious activity, market observation, contractual, issuer, investor, law-enforcement or other reporting. The FCA states that specified firms and venues must detect and report suspicious orders and transactions within its applicable regime. That requirement should not be generalised to entities or transactions outside scope.

Closure records finding, consequence, corrective action, affected parties, notifications, financial reconciliation, root cause, policy or system change, owner and effectiveness test. The historical case remains available under the retention policy.

15. Validate alert logic before trusting the dashboard

Surveillance models can fail silently. FCA Market Watch 79 describes a case in which a third-party surveillance system's news feed was not activated, preventing the model from producing alerts for more than three years. The operational lesson applies broadly: configuration and data feeds require independent testing.

Model inventory should list scenario, owner, version, purpose, data sources, rules, thresholds, exclusions, deployment date, testing, limitations and change history. Retired versions remain traceable to historical cases.

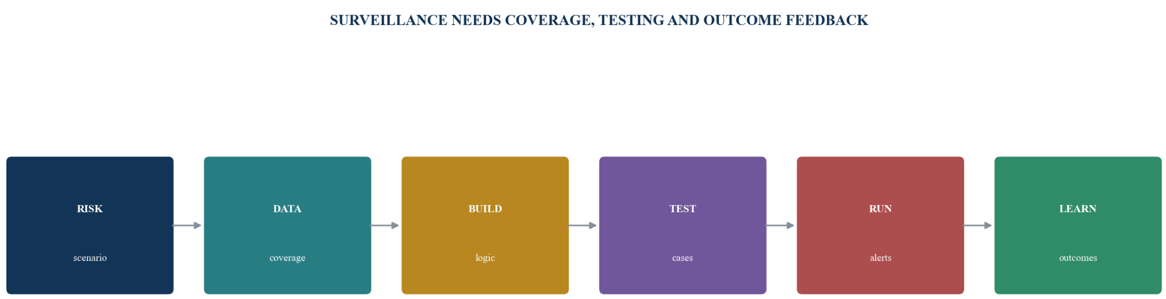
Testing includes input completeness, field mapping, timestamp quality, scenario logic, threshold boundaries, duplicate handling, access controls, alert routing and case linkage. Synthetic examples can test known conditions without relying on confidential live data.

Back-testing applies the rule to historical events and compares alerts with known outcomes. Sample review tests both alerted and non-alerted populations. A model should be challenged for missed cases and over-alerting.

Changes require approval and regression testing. A new security type, platform, geography, mandate structure, data feed or counterparty route can create gaps. Temporary exclusions should have owners and expiry.

The dashboard should expose coverage and health: events received, missing feeds, stale sources, failed jobs, alert latency, backlog, false-positive reasons and unresolved high-severity cases.

Figure 5. Surveillance model assurance cycle



Testing cadence and tolerances are illustrative management assumptions.

16. Build a decision-focused surveillance dashboard

The dashboard should answer what requires action today. It presents high-severity open alerts, transactions approaching irreversible gates, information incidents, unverified inventory, unsettled allocations and overdue cases.

Coverage metrics include active issuers, securities, inventory lots, counterparties, recipients, quotes, orders and settlements monitored. Data-quality metrics include missing identifiers, stale evidence, broken lineages, unlinked documents and feed failures.

Alert metrics include volume, rate, severity, confidence, scenario, owner, age and disposition. Case metrics include open exposure, investigation stage, findings, remediation and effectiveness testing. Trends need stable denominators.

Commercial metrics should remain evidence-led. The dashboard can show qualified opportunities, approved inventory, authorised orders, settled value, executed mandates, invoices and collected fees. It should not label circulated inventory or projected economics as revenue.

Concentration views identify repeated source holders, brokers, buyer groups, issuers, platforms, relationship owners and information recipients. These views can reveal correlated risk hidden by contact counts.

The governing body should receive decisions, consequences, owners and deadlines. Technical alert volumes belong in supporting detail.

Table 5. Decision-focused surveillance dashboard

View	Measure	Decision	Escalation signal
inventory	unique evidenced lots and active claims	controlled supply	active claims exceed evidence
access	verified routes and failed feasibility tests	permitted sharing	unresolved impossible access
information	recipients, tiers and expiry	retain or revoke access	leakage or expired access
demand	unique authorised and funded buyers	reliable book depth	duplicated or unsupported demand
settlement	finality, breaks and age	close or remediate	cash and ownership divergence
cases	high-severity exposure and backlog	investigation priority	overdue irreversible decision

Measures should use reconciled source populations and documented definitions.

17. Establish governance, privacy and retention controls

The governing body approves the risk assessment, surveillance scope, scenarios, thresholds, model inventory, case policy, information access, escalation and reporting. Business, compliance, risk, operations, technology and data owners require defined responsibilities.

Front-office information is valuable. Relationship owners often see changes in behaviour, urgency, access and market narrative before structured data does. They should escalate evidence under clear policy while remaining outside independent case decisions where conflicted.

Data use requires proportionality. Surveillance can involve personal data, communications, relationship graphs and adverse information. The organisation should establish lawful basis, notices, permitted sources, access, correction, retention, cross-border transfer and investigation holds with qualified advisers.

Sensitive cases need restricted access. A commercial team may need to know that sharing is paused without receiving confidential investigation detail or the identity behind an independent match.

Retention should support reconstruction of material decisions while avoiding indefinite accumulation. Mandates, access grants, quotes, orders, allocations, payments, settlements, alerts and cases can have different statutory and contractual requirements.

Periodic assurance should test completeness, effectiveness and independence. Findings should produce owners, deadlines and verification evidence.

18. Run a ten-day private-market surveillance diagnostic

Days one and two define the business, transaction population, entities, securities, systems, information flows, regulatory perimeter and irreversible decisions. The team maps current risk scenarios.

Days three and four reconcile issuer, security, holder, mandate, inventory and source-lineage data. Active blocks receive fingerprints and duplicate tests.

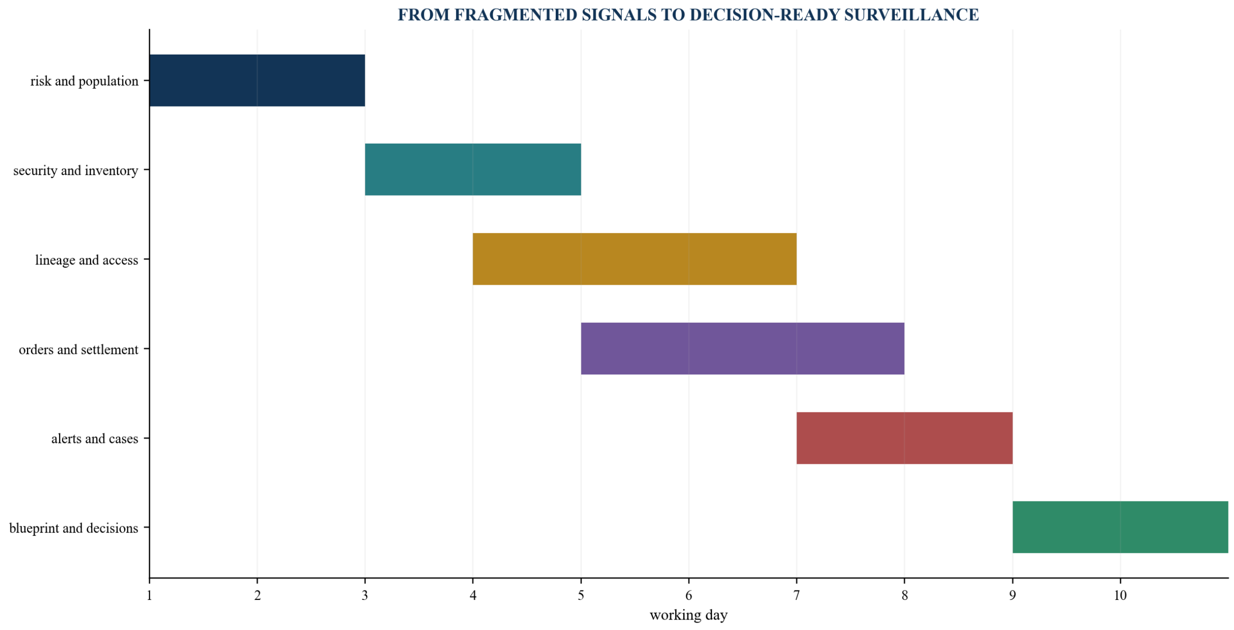
Days five and six map counterparties, recipients, access permissions, quotes, indications, orders, allocations, payments and settlements. The review tests impossible access and recycled demand.

Days seven and eight reconstruct alert-worthy historical cases, information incidents, settlement breaks and open exceptions. Data coverage and model health are assessed.

Day nine scores maturity across risk assessment, data, rules, triage, cases, testing, governance and reporting. Critical live-transaction risks receive immediate owners.

Day ten presents a board-ready surveillance blueprint, current high-risk cases, qualified inventory view, alert library, data architecture, delivery assumptions and thirty-day implementation plan.

Figure 6. Ten-day surveillance diagnostic



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

19. Implement a thirty-day surveillance control office

Days one to five establish governance, risk assessment, scope, identifiers, evidence hierarchy, stop rules, case policy and decision rights. Active high-risk blocks receive interim controls.

Days six to ten build the issuer, security, holder, mandate and inventory master. The team loads fingerprints, source lineages, document hashes and evidence expiry.

Days eleven to fifteen implement counterparty, recipient, information, quote, order, allocation, payment and settlement events. Historical data is reconciled and missing fields assigned.

Days sixteen to twenty configure duplicate inventory, impossible access, recycled demand, information, price, quantity, sequencing and settlement alerts. Test cases and thresholds are approved.

Days twenty-one to twenty-five implement triage, case files, evidence preservation, escalation, model inventory and dashboard reporting. Historical outcomes support calibration.

Days twenty-six to thirty train users, test incidents and feed failures, close critical findings, establish assurance and obtain management acceptance. Open remediation retains named owners and deadlines.

Table 6. Thirty-day surveillance-office deliverables

Workstream	Deliverable	Acceptance evidence	Owner
inventory	security, holder and lot master	sampled source reconciliation	transaction-data owner
lineage	source and access graph	convergent routes tested	surveillance owner
events	immutable quotes, orders and settlements	sequence reconstruction	operations owner
alerts	approved scenario library	positive and negative test cases	control owner
cases	triage and investigation workflow	historical case reproduced	independent reviewer
reporting	coverage, alerts, exposure and outcomes	governing pack accepted	management owner

Scope should reflect transaction volume, systems, jurisdictions and applicable regulation.

20. Package the work around urgent paid transaction outcomes

The framework can support a private-market surveillance diagnostic, duplicate-inventory remediation, source-lineage reconstruction, impossible-access review, information-leakage response, alert-library build, historical case investigation, settlement feedback programme or recurring surveillance control office.

Commercial qualification should identify the active consequence: a live block whose origin is disputed, several brokers circulating the same inventory, a buyer book with repeated identities, unauthorised information sharing, an imminent allocation, a changed payment instruction, a failed close, an audit finding or a board deadline. The economic buyer should own the decision, evidence and budget.

The engagement should define entities, securities, transactions, jurisdictions, systems, messages, data, alert scenarios, cases, decisions, deliverables, advisers, exclusions and reliance limitations. Reserved legal, regulatory, brokerage, investigation, sanctions, valuation, accounting, audit and tax functions remain with appropriately qualified and authorised providers.

Fees can reflect transaction urgency, issuer and security complexity, event volume, source-lineage depth, counterparties, historical reconstruction, data quality, model configuration, system integration and 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 collected fees requires executed mandates, valid invoices and cleared bank receipts. Pipeline, transaction value and expected economics remain management estimates.

The strongest offer connects an active risk to a defined output: unique evidenced inventory, controlled information access, credible demand, explainable alerts, resolved cases, reconciled settlement and a surveillance operating model that can support repeat execution.

References

[1] US 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] US Securities and Exchange Commission. Private Companies and the SEC. Updated 24 April 2026. https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/private-companies-sec

[3] US Securities and Exchange Commission. Risky Business: Pre-IPO Investing. https://www.sec.gov/about/reports-publications/investorpubspreipohtm

[4] Financial Industry Regulatory Authority. Private Placements. https://www.finra.org/rules-guidance/key-topics/private-placements

[5] Financial Industry Regulatory Authority. Regulatory Notice 10-22: Obligation of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings. https://www.finra.org/rules-guidance/notices/10-22

[6] Financial Industry Regulatory Authority. Regulatory Notice 23-08: Obligations When Selling Private Placements. 9 May 2023. https://www.finra.org/rules-guidance/notices/23-08

[7] Financial Conduct Authority. How to Report Suspected Market Abuse as a Firm or Trading Venue. Updated 26 February 2026. https://www.fca.org.uk/markets/market-abuse/how-report-suspected-market-abuse-firm-or-trading-venue

[8] Financial Conduct Authority. Market Watch 69: Observations on Market Abuse Surveillance. 17 May 2022. https://www.fca.org.uk/publications/newsletters/market-watch-69

[9] Financial Conduct Authority. Market Watch 79: Market Abuse Surveillance Failures. https://www.fca.org.uk/publications/newsletters/market-watch-79

[10] Financial Conduct Authority. Transaction Reporting. Updated 23 December 2024. https://www.fca.org.uk/markets/transaction-reporting

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

[12] 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

[13] Dubai Financial Services Authority Rulebook. AMI 5.11.2 Guidance: Surveillance Systems. https://dfsaen.thomsonreuters.com/entiresection/20460

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

About the Author

Chennakeshav Adya, Independent Researcher