Clean Teams that Accelerate Diligence without Creating Gun-Jumping Risk

A board framework for information classification, controlled analysis and pre-closing decision discipline

Authored by Chennakeshav Adya
Independent Researcher
September 2026

Abstract

Acquirers need enough evidence to value a target, arrange financing, plan a lawful closing and prepare for operational continuity. When the parties compete, the same diligence process can expose current prices, customer strategies, costs, product roadmaps, capacity decisions and other competitively sensitive information. Poorly controlled access can weaken independent conduct before closing, contaminate commercial decisions and create merger-control or competition-law risk. Excessive restriction can leave the board underwriting an opaque asset and delay the first hundred days.

This paper develops a clean-team operating system that connects each business question to a defined data class, permitted recipient, analytical method, release rule, decision owner and deletion obligation. It distinguishes ordinary transaction information from restricted competitive information; separates external advisers, clean-team personnel and ordinary business teams; defines aggregation and redaction thresholds; and links every output to a recorded transaction decision. Current public material from the US Federal Trade Commission and Department of Justice, UK Competition and Markets Authority, European Commission and OECD provides the regulatory foundation. Applicable duties depend on the facts, jurisdictions, contractual terms and current law.

The worked case is wholly hypothetical. A diversified industrial technology group considers acquiring a direct competitor for an assumed enterprise value of USD 1.85 billion. The parties identify 420 diligence requests, of which 135 contain potentially sensitive commercial content. Twelve approved clean-team members produce 34 decision-use outputs from restricted material. The paper models a USD 1.80 million control programme against an assumed USD 190 million present value of gross transaction synergies. Every company, amount, timetable and outcome is a scenario assumption. Live transactions require current competition, corporate, financing, data-protection, employment and sector-specific advice in every relevant jurisdiction.

JEL Classification: G34, K21, K42, L40, M15

Keywords: clean teams, gun jumping, merger control, due diligence, competitively sensitive information, access controls, data aggregation, integration planning, antitrust

1. Treat information access as a transaction decision

A clean team is a controlled mechanism for answering legitimate transaction questions without giving operating personnel unrestricted access to a competitor's sensitive information. Its purpose is decision quality. It should allow the board, financing sources and authorised advisers to evaluate value, risk, separability, regulatory exposure and closing readiness while the parties continue to compete independently.

The control challenge begins with the question being asked. “Show us the customer file” is too broad. “Estimate the proportion of revenue subject to change-of-control consent, using customer identities only where counsel determines that identity is necessary” creates a defined analytical purpose. The purpose determines which fields are needed, who may see them, which calculations may be performed and what can be released to the deal team.

Transaction leaders should reject two weak operating models. The first puts nearly all information into an ordinary virtual data room and relies on confidentiality language alone. The second blocks access so comprehensively that the investment case depends on management assertions that cannot be tested. A functioning design classifies information, assigns it to a controlled lane and records how the resulting analysis informs a specific decision.

The board should approve the clean-team mandate alongside the diligence plan. The mandate should define the transaction purpose, participating entities, applicable jurisdictions, restricted categories, approved members, prohibited uses, release authority, recordkeeping, incident response and termination. It should also state that the parties remain independent before closing and that no clean-team process authorises operational coordination.

The central governance artefact is an information decision register. Each entry records the business question, requested fields, sensitivity class, legal basis, source owner, approved recipients, transformation method, output recipient, decision supported, retention period and final disposition. This creates traceability from raw information to board action.

2. Start from the standstill principle

Public guidance consistently reflects a basic pre-closing principle: merging parties remain separate businesses until the legal conditions for control have been satisfied. The US Federal Trade Commission has warned that parties must continue to act independently before consummation and should take special care with current or future prices, strategic plans and costs. The agency identifies clean teams and third-party consultants as tools for controlling sensitive diligence. [1]

The 2023 US Merger Guidelines explain that access to a rival's competitively sensitive information may undermine competition or facilitate coordination. The relevance of this principle extends beyond a filing timetable because the information exchange itself can affect market conduct. [2] The US Department of Justice has stated publicly that potential gun-jumping conduct may trigger a separate investigation. [3]

The OECD's background note on gun jumping similarly discusses aggregation, redaction, historic information, counsel review and clean teams as possible safeguards. It emphasises that parties remain independent and notes that information exchange can also raise concerns under rules governing coordination between competitors. [4]

The UK CMA has used interim measures, derogations and enforcement action to preserve independent operation and control information flows. A public clean-team agreement in the Ladbrokes and Coral investigation restricted the permitted purpose, representatives and use of confidential information. [5] A later CMA derogation letter required defined clean-team members, confidentiality obligations, firewalls, access restrictions, controlled summaries and records. [6]

These sources do not create a single universal template. They establish practical design disciplines. A transaction needs a jurisdiction map, current advice and a control environment that reflects the sensitivity of the information and the recipients' ability to influence competition.

Table 1. Public principles and transaction-control implications

Source	Public principle	Transaction-control implication	Evidence to retain
FTC competition guidance	Parties must remain independent before closing; sensitive information requires special care	Use counsel-vetted recipients, separate protocols, controlled storage and reviewed outputs	Approved-member list, protocol, access logs and release approvals

Source	Public principle	Transaction-control implication	Evidence to retain
2023 US Merger Guidelines	Access to competitively sensitive rival information can undermine competition or facilitate coordination	Treat access risk as part of the substantive competition analysis	Sensitivity assessment, recipient-role analysis and mitigation record
OECD gun-jumping note	Aggregation, redaction, historic data and clean teams may reduce risk	Select the least sensitive dataset capable of answering the decision question	Field-level data specification and transformation record
UK CMA public measures	Purpose limits, defined representatives, firewalls, reviewed summaries and records can support controlled access	Align the clean-team design with any order, undertaking or authority consent	Order matrix, derogation terms, monitoring evidence and incident log
European Commission confidentiality tools	Data rooms and confidentiality rings restrict access and use while enabling necessary disclosure	Separate authority disclosure controls from commercial diligence controls and reconcile both	Data-room rules, confidentiality acknowledgements and disclosure index

The table summarises selected public materials. It does not state the complete legal test in any jurisdiction.

3. Define the decisions before requesting the data

Diligence expands when requests are organised by function rather than decision. Commercial teams ask for customers, finance asks for margins, operations asks for capacity and integration teams ask for systems. The target receives overlapping requests, sensitivity escalates and the clean team becomes a document-routing service.

A decision-led model begins with the board and transaction committees. Each decision should have an owner, date, threshold and evidence requirement. Typical decisions include maximum price, synergy confidence, financing capacity, signing conditions, regulatory strategy, separation feasibility, customer-consent plan and Day 1 continuity. The clean team then works backwards to the minimum information needed.

Consider customer concentration. The board may need to know whether the top twenty relationships account for more than an agreed share of contribution, whether material contracts contain change-of-control rights and whether a forecast depends on uncontracted renewals. The first pass may use anonymised customer identifiers, revenue bands, contribution bands, contract-expiry buckets and consent flags. Identity can remain restricted unless it becomes necessary for a defined consent or regulatory question.

The same logic applies to pricing. A synergy model may need price dispersion, discount leakage and contract-indexation exposure. It rarely requires ordinary commercial staff to see a competitor's current customer-by-customer prices. A clean team can calculate weighted averages, distributions, cohorts and anonymised outliers, then release an approved conclusion with the methodology and uncertainty.

Every request should state the counterfactual. What would the decision-maker do if the information were unavailable? What threshold would change the decision? If no answer changes the transaction, price, financing, condition, covenant, remedy or implementation plan, the request may be curiosity rather than diligence.

4. Build a five-class information taxonomy

A clean team needs a taxonomy that transaction participants can apply consistently. Legal labels alone are insufficient because sensitivity depends on content, age, granularity, market context and recipient role. The proposed taxonomy has five classes.

Class 1 is public information. It includes published accounts, public filings, websites, public tenders and properly available market material. Public status should be verified because material shared with selected counterparties is not necessarily public.

Class 2 is ordinary confidential transaction information with limited competitive sensitivity. Examples may include corporate structure, historical audited statements, property documents, litigation summaries and policies. Access remains subject to the transaction agreement and data-room controls.

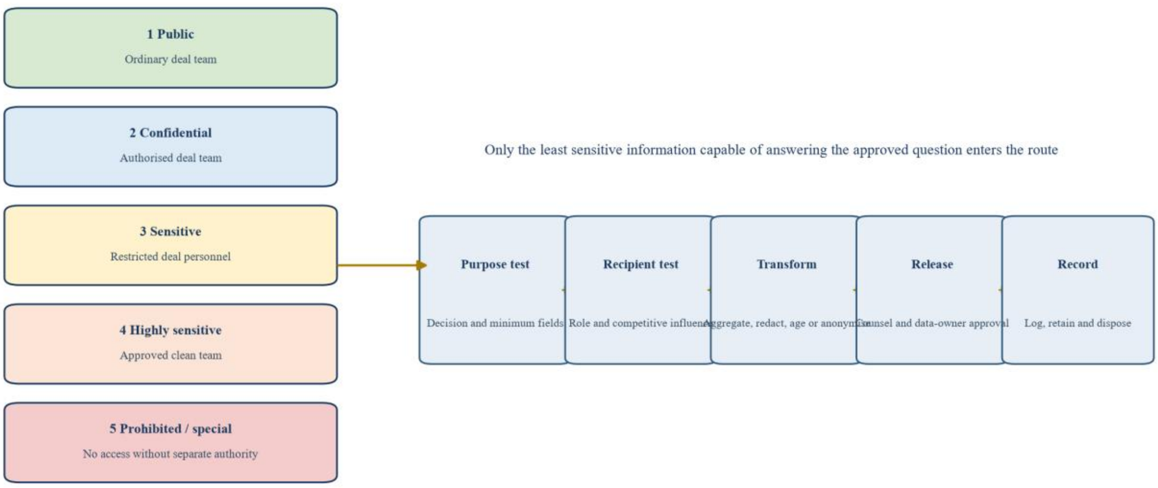
Class 3 is commercially sensitive information that may be shared only with defined deal personnel or advisers. It can include detailed historical performance, customer terms, procurement arrangements and operating metrics. The classification depends on whether recipients can influence current competitive decisions.

Class 4 is highly sensitive competitive information. Current or forward-looking prices, named-customer strategies, product roadmaps, bidding intentions, unit costs, capacity changes, innovation plans and employee-specific commercial data often belong here. Access should be restricted to an approved clean team, with transformed outputs released only after review.

Class 5 is prohibited or specially controlled information. It covers material that the governing protocol, law, order, contract or authority direction does not permit to be shared, as well as information whose purpose is not legitimate or whose risk cannot be controlled. It can also include privileged material, export-controlled data, personal data or sector-regulated information requiring a separate legal route.

Classification should occur at field or document-section level where practical. A board paper may contain public market data, ordinary confidential financials and forward-looking pricing strategy. Treating the whole document as one class either exposes sensitive content or blocks useful evidence.

Figure 1. Information-classification and routing architecture



The architecture is a proposed governance model. Applicable restrictions require transaction-specific advice.

5. Separate roles according to competitive influence

Clean-team membership should be based on function and influence, not seniority or convenience. A person who sets current price, decides bids, allocates capacity, manages key customers or determines product strategy may create greater risk than an external analyst. A senior executive may also be unable to forget sensitive information after a deal is abandoned.

The operating model can use four rings. Ring A consists of external legal advisers and other advisers specifically engaged for the controlled review. Ring B consists of approved internal personnel who do not participate in relevant day-to-day competitive decisions and who accept enhanced restrictions. Ring C consists of the ordinary transaction team, which receives reviewed outputs. Ring D consists of operating personnel who receive only the decisions, assumptions or implementation tasks needed to continue lawful planning.

The clean-team protocol should list named people, employers, roles, permitted repositories and expiration dates. Substitution should require documented approval. Generic access for “finance,” “strategy” or “integration” creates ambiguity and makes access review unreliable.

Recipient analysis should consider reporting lines. An internal analyst may not set price directly but may prepare the analysis used by the pricing committee. A corporate development executive may later return to a commercial role. An operating consultant may serve both parties in the market. The protocol should address these pathways, cooling-off periods where appropriate, and post-termination handling.

Each member should receive training on the permitted purpose, prohibited discussions, handling rules, output controls, incident escalation and continuing obligations if the transaction ends. A signed acknowledgement supports accountability but does not replace technical controls.

Table 2. Proposed data classification and access matrix

Information type	Typical sensitivity	Initial recipient	Permitted analytical output	Ordinary business recipient
Public filings and published market data	Low	Deal team	Source-linked analysis	Yes
Historical audited financial statements	Moderate	Authorised deal team	Reconciled trend and quality-of-earnings analysis	Defined transaction personnel
Named-customer current pricing and discounts	High	Approved clean team	Anonymised distribution, weighted averages and threshold exceptions	Reviewed aggregate only
Customer strategy, active bids and renewal intentions	Very high	External or strictly ring-fenced clean team	Risk bands and decision conclusions with identities withheld	No raw access before closing
Unit cost, supplier terms and capacity plans	High	Approved clean team	Indexed cost curve, concentration and capacity scenarios	Reviewed aggregate only
Product and innovation roadmap	High	Approved subject-matter clean team	Capability map and milestone-risk summary	Need-to-know reviewed conclusion
Personal data, privileged material or controlled technical data	Special	Separate authorised process	Only the output permitted by applicable law and protocol	As specifically authorised

Recipient suitability depends on the transaction, market, jurisdiction and applicable orders.

6. Specify the minimum dataset

Data minimisation is a diligence discipline. The clean team should create a field specification before the target uploads material. It should identify the source system, period, unit, currency, definitions, transformations and permitted joins. This reduces repeated requests and limits the amount of sensitive information processed.

Age is a control variable. Historical information may be less sensitive than current or forward-looking information, although the answer depends on the market. In a stable long-term contract business, older customer economics may remain competitively informative. In a rapidly changing spot market, recent capacity and bids may be especially sensitive. The protocol should define time bands by information category rather than adopting one universal cut-off.

Granularity is another control. A decision may be answered with monthly cohorts instead of transactions, regions instead of sites, product families instead of stock-keeping units, and customer bands instead of names. The clean team should test whether the transformation preserves the analytical signal. An aggregate that conceals concentration or volatility can mislead the board.

Redaction removes fields that are unnecessary for the analysis. Pseudonymisation replaces identity with a stable code so records can be linked without revealing the customer or supplier. Aggregation combines observations. Binning converts precise values into ranges. Top- and bottom-coding limits extremes. Noise or statistical privacy methods may be relevant for some datasets, but they require careful validation because they can distort transaction conclusions.

The minimum dataset should also include quality fields. Source, extraction time, completeness, manual adjustments and reconciliation status allow the clean team to distinguish an analytical result from an unsupported data dump. Sensitive data with poor lineage creates legal risk without delivering reliable diligence.

7. Design the clean-room technology as a control system

A separate folder with restricted permissions is only the beginning. The technology design should enforce the protocol and produce evidence that the controls operated. Core features include named accounts, multifactor authentication, least-privilege roles, expiry dates, immutable logs, watermarking, download restrictions, device controls, encryption and rapid revocation.

The repository should be logically separated from ordinary transaction storage. The FTC has cautioned against storing clean-team information on share drives accessible to operating employees. [1] Restricted files, working analyses and release-ready outputs should occupy different locations. A released output should carry a version, approver, date, recipients and permitted purpose.

Analytical work may require a controlled environment where data can be queried without raw export. The design can disable copy, print and external transfer; permit only approved code or tools; log queries; and route outputs to a release queue. These features should be proportionate to the sensitivity and the team's technical capability.

Access review should be continuous. A person who changes role, leaves the deal, joins an operating committee or becomes conflicted may no longer be suitable. Automated expiry reduces forgotten access. Weekly recertification may be appropriate in an accelerated process, while a long review may require a formal monthly certification.

Backups, incident response and deletion also matter. The protocol should identify where derived data, temporary files, email attachments, chat messages and local caches can exist. Final disposition should cover all copies that the parties control, subject to legal hold and professional-retention duties. A certificate of return or deletion should state the scope and exceptions.

8. Create a controlled analytical factory

The clean team should operate like a small analytical factory. Inputs enter through a documented intake. Analysts validate the schema and reconcile totals. Approved methods produce working outputs. A reviewer tests the result. Counsel and the information owner assess whether the output can be released. The recipient receives a decision-use product with limitations and a version number.

Standard output types improve speed. A customer-concentration output might show revenue and contribution by anonymised band, contract-expiry buckets, consent flags and concentration sensitivity. A pricing output might show indexed price distributions by product family and geography, excluding named customers and current bid intentions. A capacity output might show utilisation ranges and approved scenarios rather than site-level future actions.

The reviewer should ask whether the output allows reverse engineering. A small cohort, an obvious outlier or a well-known contract can reveal identity even without a name. Combining several released outputs may also expose information that each output conceals alone. The release log should therefore show related outputs and cumulative disclosure.

Quality control should test definitions, arithmetic, reconciliations, sample sizes, missing data, outliers and scenario assumptions. The output should distinguish observed records from management estimates and transaction assumptions. It should state the period and whether the conclusion can support valuation, financing or implementation.

An efficient clean team builds reusable query templates, classification rules, output formats and review checklists. Reuse should never bypass the transaction-specific purpose or current legal review. It improves cycle time by removing avoidable drafting and data-engineering work.

Figure 2. Hypothetical diligence funnel from requests to board decisions

All counts are scenario assumptions for the worked case.

9. Release conclusions, not competitive playbooks

The clean team's output should answer the approved question without giving recipients a competitor's operating playbook. This requires judgment. A conclusion that the target's gross margin is below a stated threshold may support valuation. A file containing product-level future prices and customer negotiation positions can influence current competition.

Each release should contain five elements: the question, the permitted conclusion, the method, the limitations and the decision implication. The team should avoid attaching raw extracts unless the recipient is approved for that class. Where a numeric output remains sensitive, a threshold answer, index, band or scenario may be sufficient.

Counsel review should be substantive. The reviewer needs to understand the market context, recipient role and analytical content. Removing names may not be enough. A dataset showing one customer in a country, one supplier for a component or one bid in a month can be identifiable.

Release decisions should also reflect timing. Information appropriate after public announcement may remain inappropriate before signing. Information appropriate after clearance may still be restricted until closing. A regulator's interim order may create a separate control period. The access matrix should therefore link permissions to transaction milestones.

The output owner should confirm how the recipient may use the information. A valuation committee may use a clean-team conclusion to adjust price. An integration planner may use a capability count to estimate resourcing. An operating team should not use the output to change current pricing, bids, customers, suppliers, output or innovation plans before closing.

10. Keep integration planning capability-based

Integration planning creates particular pressure for detailed information. Leaders want Day 1 organisation charts, customer plans, supplier consolidation, product rationalisation, pricing harmonisation and system migration. Some preparation is necessary for a lawful and orderly closing. Certain actions or information flows can compromise independent conduct.

A safer planning model is capability-based. Before closing, the integration team can define governance, decision calendars, workstream structures, generic Day 1 controls, data-migration methods, communication templates and contingency plans. It can use clean-team outputs to estimate scale and complexity without directing the target's current operations.

Plans should contain closing gates. Actions involving customers, prices, suppliers, employees, capacity, products or systems should state the legal trigger and authorised owner. The plan should identify tasks permitted before signing, after signing, after clearance and only after closing. This turns legal advice into an executable workplan.

Clean-team members can prepare a sealed implementation pack for release after the relevant condition is satisfied. The pack may contain validated mappings, issue lists and detailed analyses that ordinary operating personnel could not receive earlier. Access should change through an approved release event, rather than through an informal assumption that clearance or signing has occurred.

The integration management office should maintain a dependency register connecting each initiative to information, authority, customer or regulatory prerequisites. This prevents a workstream from using a clean-team output outside its approved purpose.

11. Protect independent decision-making

Information controls work only when decision rights remain separate. The acquirer should not approve the target's ordinary pricing, bids, customers, suppliers, hiring, product releases or capacity decisions before it lawfully controls the business. Contractual protections for extraordinary conduct require careful design and current advice; they should not become operational control.

The parties should maintain separate meetings for current competitive decisions. Joint transaction meetings should have agendas, approved attendees and minutes. If a discussion enters restricted territory, participants should stop, record the issue and route it through the clean-team process.

Communication controls are essential during accelerated diligence. Senior leaders may speak frequently and bypass repositories. The protocol should cover email, messaging, calls, workshops and informal conversations. Clean-team information should not be pasted into broad chat channels or management decks.

Transaction teams should distinguish preparation from implementation. Drafting a post-closing pricing-governance policy may be preparation. Agreeing current prices, dividing customers or coordinating bids before closing would create a fundamentally different risk. The applicable conclusion depends on facts and law; the governance system should force the question before the action.

The target should retain its own management authority. It should document material decisions in the ordinary course and record any transaction-consent request. This protects both parties by showing who decided, under which contractual provision and for what reason.

12. Integrate the clean team with valuation and financing

A clean team should improve the investment case, not sit beside it. Its outputs need defined model destinations. Customer-quality analysis may change revenue retention assumptions. Price and contribution analysis may change margin normalisation. Capacity evidence may change capital expenditure. Contract analysis may affect debt sizing and conditions precedent.

The valuation model should identify cells informed by clean-team outputs and preserve the output version. If a release changes, the model owner should assess the effect. A board paper should not cite a conclusion that has been superseded or whose limitations were removed in summary.

Financing sources may require information that is sensitive. Their advisers and information barriers should be addressed in the protocol and transaction documents. A lender's commercial team should not automatically receive raw competitor data. Approved outputs can support lender diligence, covenant design and credit approval while respecting the information controls.

The hypothetical case assumes USD 190 million present value of gross synergies. Clean-team analysis supports only part of that amount. Management distinguishes evidence-supported synergy, management estimate and strategic option value. The investment committee applies separate probability, timing and implementation-cost assumptions. This avoids converting restricted data into an unjustified synergy uplift.

The control programme also has a direct cost. External advice, secure technology, analysts, target extraction work and review time are assumed to cost USD 1.80 million. That amount should be evaluated against the value of better pricing, financing certainty, regulatory discipline and closing readiness. The comparison remains a scenario, not evidence that every transaction requires the same spend.

Table 3. Hypothetical cost, timing and decision-value scenario

Item	Scenario assumption	Decision use	Control implication
Enterprise value	1,850.0	Price and financing	Board-level evidence threshold
Gross synergy present value	190.0	Strategic value case	Separate supported, estimated and optional components
Clean-team programme cost	1.8	Transaction cost and resourcing	Stage spend against decision gates
Total diligence requests	420	Workload planning	Deduplicate by transaction decision
Potentially sensitive requests	135	Restricted-workload planning	Apply field-level classification
Approved clean-team members	12 people	Capacity and segregation	Named access with role review and expiry
Released decision-use outputs	34	Board, finance and workstream decisions	Versioned release and cumulative-disclosure review
Planned signing-to-closing period	120 days	Timetable	Milestone-based permissions and sealed Day 1 pack

All amounts and timings are scenario assumptions. USD millions unless stated otherwise.

13. Govern advisers, counterparties and financing sources

The clean-team perimeter can include lawyers, accountants, consultants, investment banks, financing sources, insurers, trustees, regulators and technology providers. Each recipient should have a defined purpose and contractual basis. A recipient's professional status does not make every information flow appropriate.

Adviser engagement letters and confidentiality arrangements should align with the transaction protocol. They should address permitted use, onward disclosure, personnel, conflicts, security, incident reporting, retention and return or deletion. Where advisers operate across practices or clients, the transaction should consider information barriers and role conflicts.

The target remains the owner of its information unless the governing arrangements state otherwise. It should know what enters the restricted environment and which outputs are proposed for release. Release review should avoid allowing the target to manipulate legitimate diligence conclusions, while preserving its ability to identify sensitivity or factual error.

Financing sources need a controlled disclosure path. The acquisition-finance team may need sufficient evidence for credit approval, syndication and documentation. The protocol should identify whether lenders receive raw material, adviser reports or approved summaries. Any syndication or investor disclosure needs separate attention because the recipient group can expand.

Regulatory submissions may require detailed evidence. The authority process should be governed by the applicable procedural rules and confidentiality arrangements. The European Commission publishes information on data rooms and confidentiality rings used to allow restricted access to necessary material. [7][8] Those mechanisms serve a regulatory process and should be coordinated with, rather than assumed identical to, the parties' commercial diligence clean team.

14. Measure the process with leading indicators

The transaction committee needs operating metrics that show whether diligence is moving and controls are working. A simple request count is inadequate. The dashboard should connect throughput, decision coverage, sensitivity and control health.

Useful throughput measures include median time from request to classification, time from complete data receipt to analysis, time from output submission to release decision, and requests returned for unclear purpose. Decision measures include board questions answered, model assumptions supported and unresolved high-value uncertainties.

Control measures include active approved members, overdue access recertifications, restricted downloads, unapproved sharing attempts, outputs awaiting review, cumulative-disclosure flags, incidents and disposition completion. Quality measures include reconciliation exceptions, missing definitions, sample-size limitations and outputs replaced after validation.

Targets should not reward disclosure volume. A team can appear fast by releasing material that should remain restricted. Measures should reward decision resolution and compliant cycle time. An output that answers one major underwriting question can be more valuable than fifty uploaded documents.

The dashboard should distinguish a process delay from a substantive uncertainty. If the target has not extracted data, the action is operational. If the data show unstable customer economics, the issue belongs in valuation and transaction terms. Clear ownership prevents the clean team from becoming the holding area for unresolved commercial decisions.

15. Use a formal output-release decision

Every material output should pass a release decision with recorded answers. First, does the output answer an approved transaction question? Second, is each field necessary? Third, can the recipient influence current competition? Fourth, can identity or strategy be reverse engineered? Fifth, do combined prior releases change the risk? Sixth, do an order, undertaking, contract or law impose additional restrictions?

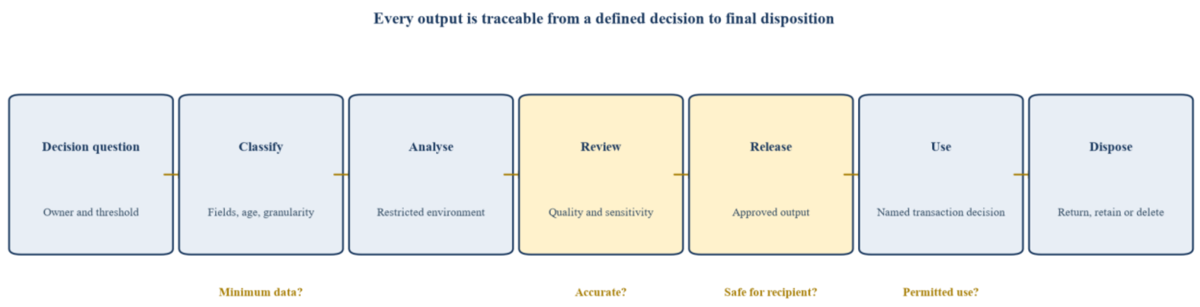
The release authority may consist of competition counsel, the target information owner and a clean-team lead. Some transactions may require a monitoring trustee or authority consent. The protocol should resolve disagreements and identify who can stop a release.

Outputs should be marked by class and permitted recipient. A short cover sheet can state the analytical period, sources, transformations, assumptions, limitations, approvers and prohibited uses. If the output is revised, the repository should withdraw or supersede the old version where possible.

Urgency should not bypass the gate. The protocol can define an expedited review for financing deadlines or board meetings, with the same substantive tests and a complete record. Repeated emergency requests may indicate poor decision planning.

If an output cannot be released, the clean team should consider whether a less detailed answer works. It may provide a yes-or-no threshold, range, indexed result, anonymised cohort, scenario or counsel conclusion. If no safe form answers the question, the decision-maker should see the uncertainty and adjust price, terms or risk appetite.

Figure 3. Clean-team operating workflow and decision gates



The workflow is a proposed control sequence.

16. Prepare for incidents before they occur

An incident can include access by an unapproved person, a misdirected email, an over-detailed output, use outside the permitted purpose, an exposed device, a prohibited discussion or a failure to revoke access. The response plan should be ready before the first restricted file arrives.

The first actions are containment and preservation. Access may need to be suspended, links revoked and recipients instructed not to use or forward material. Logs, messages and versions should be preserved. The response team should identify the information, recipients, timing, access and actions taken.

Assessment requires legal, technical and transaction input. The team should evaluate competition risk, contractual duties, orders, personal-data obligations, privilege, cybersecurity and the effect on regulatory submissions. Notification decisions depend on applicable requirements and current advice.

Remediation can include deletion confirmation, recipient recusal, additional barriers, revised outputs, training, protocol amendment, authority engagement and changes to transaction governance. The team should also determine whether a tainted recipient can continue in a commercial role or whether the information affects independent decisions.

Incident metrics should be reported with context. A blocked access attempt can show that a control worked. An unreported disclosure discovered weeks later indicates a different problem. The committee should focus on containment, consequence and recurrence risk.

17. Learn from public enforcement signals

Public cases show the commercial importance of disciplined information controls. The CMA announced fines of almost GBP 5 million in relation to breaches of an interim enforcement order during its JD Sports and Footasylum investigation. Its release described the sharing of commercially sensitive information by chief executives and deficiencies in policies and safeguards, together with reporting failures. [9]

The case does not mean that every information exchange produces the same outcome. It demonstrates why seniority, informal communication and weak policy execution deserve attention. A clean-team process that covers only the data room leaves executive conversations unmanaged.

The European Union's Illumina/GRAIL proceedings and the Court of Justice's Altice judgment are part of the broader body of public material on implementing transactions before clearance. [10][11] Transaction teams should obtain current advice on the relevance of any case to their facts and jurisdiction.

Competition authorities also enforce sensitive information exchange outside mergers. The CMA's 2025 financial-services decision reported fines exceeding GBP 100 million in a case involving exchanges of competitively sensitive information. [12] The fact pattern differs from clean-team diligence, yet it reinforces that recipient, purpose and market effect matter.

The practical response is an evidence-based control system. Policies should be translated into named access, technical restrictions, reviewed outputs, meeting controls, incident escalation and audit evidence. Leadership should receive training before sensitive discussions begin.

18. Calibrate the control to the risk

Every transaction does not need the same clean-team structure. Proportionality begins with the relationship between the parties. Direct competitors with overlapping customers, products and bids create a different risk from businesses in separate markets. Vertical relationships can still expose input costs, customer strategies, capacity or foreclosure-relevant information.

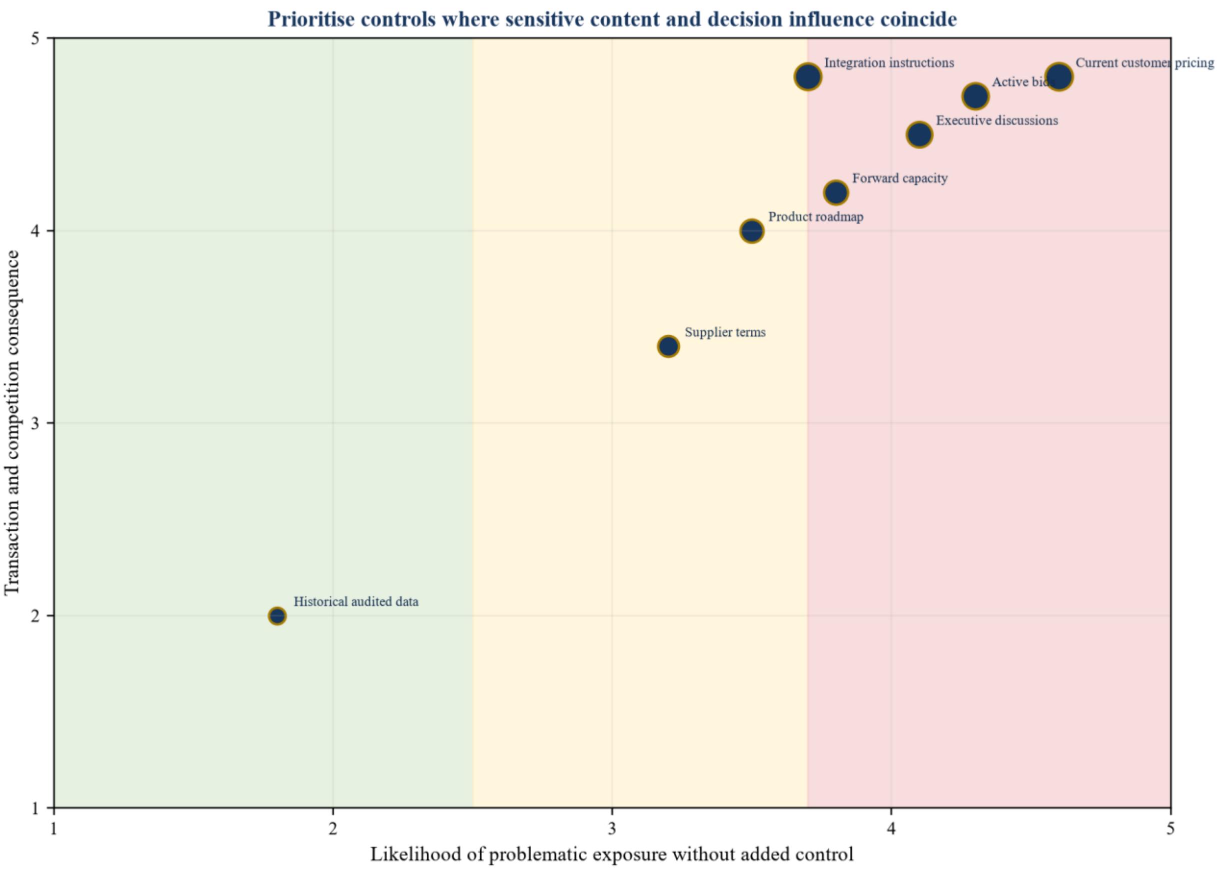
The assessment should consider market concentration, information age, granularity, volatility, transaction stage, recipient role, deal probability and the possibility that the transaction fails. It should also consider whether a public order or authority measure governs conduct.

A tiered approach can scale controls. A low-sensitivity lane may use an ordinary data room and standard confidentiality. A moderate lane may restrict access to named deal personnel. A high-sensitivity lane may require a separate clean team, controlled analytics and counsel-reviewed outputs. A special lane may require external-only review, trustee involvement or authority consent.

The design should be revisited as the transaction changes. New overlap findings, regulatory intervention, a longer timetable, a changed bidder, additional financing sources or a failed deal can alter the risk. Access should not expand automatically because the team has become familiar with the process.

The decision record should explain why the selected control is sufficient. This supports governance and allows the team to identify assumptions that require monitoring.

Figure 4. Hypothetical gun-jumping and information risk heat map



Likelihood and consequence scores are scenario assumptions before additional controls.

19. Implement the system in four phases

Phase 1 establishes governance before sensitive diligence. The transaction sponsor appoints the clean-team lead. Counsel maps jurisdictions, standstill obligations, contractual restrictions and any authority measures. The team defines decisions, taxonomy, roles, technology, release authority and incident response. The target validates extraction routes.

Phase 2 pilots the process. A small set of high-value questions tests classification, upload, analysis, review and release. The pilot should include one difficult dataset and one senior decision. Lessons are incorporated before the main diligence wave.

Phase 3 scales controlled analysis. Requests are deduplicated, prioritised by decision value and assigned to analysts. Dashboards track throughput, unresolved questions and controls. The clean team prepares approved outputs for valuation, financing, regulatory work and gated integration planning.

Phase 4 manages transaction milestones and disposition. Permissions are reassessed at signing, public announcement, clearance and closing. A sealed implementation pack is released only when authorised. If the transaction closes, relevant information moves into the combined-business governance. If it fails, the parties execute return, deletion, recusal and continuing-obligation steps.

Independent assurance may be appropriate for a complex or high-risk transaction. A reviewer can test membership, permissions, samples of releases, logs, incidents and disposition evidence. The scope should support the board's needs and any formal obligations.

Table 4. Proposed implementation roadmap and accountability

Phase	Core actions	Accountable owner	Gate evidence
1. Mobilise	Map decisions, jurisdictions, information classes, members, systems and incident response	Transaction sponsor and competition counsel	Approved charter, role list, data map and protocol
2. Pilot	Test intake, restricted analysis, output review and recipient use	Clean-team lead	Pilot report, control exceptions and revised workflow
3. Scale	Prioritise requests, run analyses, release outputs and maintain dashboards	Diligence lead	Decision register, release log, access certification and issue log
4. Transition or exit	Apply milestone permissions, release sealed packs, revoke access and complete disposition	Closing lead or termination lead	Closing authorisation or deletion and retention certificate

Timing should be adapted to the transaction and regulatory process.

20. Give the board a concise decision pack

The board should receive a clean-team report that supports transaction judgment without exposing restricted detail. The report should state the decisions addressed, material findings, limitations, unresolved questions, incidents, access status and impact on value, financing, conditions and implementation.

The report should explain which conclusions derive from observed records, management estimates and transaction assumptions. It should identify where aggregation or withholding limits precision. If a result could change materially after closing, the board should see the range and the contingency.

The board should ask whether the clean team has answered the questions that change price or terms, whether the transaction remains executable under the unresolved uncertainties, whether the parties remain operationally independent and whether the control environment can last through the expected timetable.

The board should also consider the failed-deal case. If the transaction does not close, what sensitive information has crossed the perimeter, who received it, what decisions can those people influence and which restrictions continue? This question should affect membership from the start.

The final approval record should identify the clean-team outputs used in the investment case. This allows later review of whether the model and integration plan relied on controlled evidence consistently.

21. Recognise the limits of the framework

This framework cannot determine whether a particular information exchange, covenant, planning activity or transaction step is lawful. That conclusion depends on the facts, relevant markets, recipient roles, jurisdictions, filing regimes, orders, transaction documents and current law.

A clean team does not cure an illegitimate purpose. It cannot authorise coordination of current market conduct or implementation of control before the applicable legal conditions are met. It also does not replace privacy, cybersecurity, privilege, export-control, employment, securities or sector-regulatory analysis.

Aggregation and anonymisation have limits. Small samples and distinctive observations may remain identifiable. Analytical outputs may become sensitive when combined. Technical controls cannot prevent every off-platform conversation or misuse.

The hypothetical case illustrates governance and economics. Its amounts, schedule, request counts, risk scores and outcomes are not market benchmarks. Management should build transaction-specific assumptions and preserve their basis.

Public guidance can change. The team should verify current official sources and obtain jurisdiction-specific advice before relying on any practice described in this paper.

22. Adopt ten operating rules

First, define the transaction decision before requesting data. Second, collect the minimum fields capable of answering that decision. Third, classify content by sensitivity, age, granularity and recipient influence. Fourth, name every approved member and review role changes.

Fifth, separate restricted data, working analysis and released outputs. Sixth, require a substantive release decision and assess cumulative disclosure. Seventh, keep pre-closing integration capability-based and place implementation behind explicit gates. Eighth, connect outputs to valuation, financing and transaction terms through version control.

Ninth, prepare for incidents, failed deals and final disposition before the first sensitive upload. Tenth, preserve evidence that the process operated: approvals, access, logs, transformations, releases, decisions and deletion or retention.

These rules turn the clean team from a confidentiality label into an operating system. The result should be faster resolution of high-value questions, clearer uncertainty and stronger control over how competitor information enters transaction decisions. The board can then evaluate the acquisition with a better evidence base while management preserves independent conduct until control may lawfully transfer.

Frequently asked questions

What is a clean team in M&A diligence?

A clean team is a defined group permitted to review restricted information for an approved transaction purpose under enhanced legal, contractual and technical controls. It produces reviewed outputs for authorised decision-makers rather than giving ordinary operating teams unrestricted access to raw competitor information.

Does a clean-team agreement make every information exchange lawful?

No. Purpose, content, recipient, market context, timing, jurisdiction and actual use remain relevant. A clean-team protocol is one control within a transaction-specific legal and governance framework.

Who should be excluded from a clean team?

People who influence current pricing, bids, customers, suppliers, capacity, product strategy or other competitive decisions often require exclusion or stronger restrictions. Suitability depends on the facts and current advice.

Can integration planning begin before closing?

Preparatory planning may be possible, subject to applicable law and transaction-specific advice. Actions that implement control or coordinate current competitive conduct should remain behind clearly documented legal and closing gates.

How should customer information be shared?

The process should begin with the decision question and use the least sensitive data capable of answering it. Anonymised identifiers, bands, cohorts and reviewed conclusions may support diligence while raw identities, current prices and negotiation strategies remain restricted.

What should an approved clean-team output contain?

It should state the question, conclusion, method, source period, transformations, limitations, approvers, recipients, permitted use and version. Raw supporting data should remain in the restricted environment unless separately authorised.

What happens if the transaction fails?

The parties should follow the agreed return, deletion, retention, recusal and continuing-confidentiality process. Access should be revoked promptly, final disposition recorded and the competitive roles of exposed recipients reassessed.

How can a board monitor whether the clean team is effective?

The board or transaction committee can monitor decision coverage, cycle time, unresolved high-value questions, access certifications, output reviews, incidents and disposition. Measures should focus on compliant decision resolution rather than document volume.

References

[1] US Federal Trade Commission, Avoiding antitrust pitfalls during pre-merger negotiations and due diligence, 20 March 2018, https://www.ftc.gov/enforcement/competition-matters/2018/03/avoiding-antitrust-pitfalls-during-pre-merger-negotiations-due-diligence

[2] US Department of Justice and Federal Trade Commission, Merger Guidelines, 18 December 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/2023_merger_guidelines_final_12.18.2023.pdf

[3] US Department of Justice, Deputy Assistant Attorney General Andrew Forman Delivers Remarks at the ABA, archived remarks, https://www.justice.gov/archives/opa/speech/deputy-assistant-attorney-general-andrew-forman-antitrust-division-delivers-remarks-aba

[4] OECD, Suspensory Effects of Merger Notifications and Gun Jumping, 2018, https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/03/suspensory-effects-of-merger-notifications-and-gun-jumping_9a7a81c3/f1ee76ef-en.pdf

[5] UK Competition and Markets Authority, Clean Team Agreement; Ladbrokes and Coral, 2016, https://assets.publishing.service.gov.uk/media/578cf1fced915d622c00012e/interim-undertakings-ladbrokes-coral.pdf

[6] UK Competition and Markets Authority, Clean Team Derogation, 8 February 2023, https://assets.publishing.service.gov.uk/media/64ee05186bc96d000d4ed23b/8_Feb_Clean_Team_Derogation_.pdf

[7] European Commission, Data rooms and confidentiality rings, https://competition-policy.ec.europa.eu/index/data-rooms-and-confidentiality-rings_en

[8] European Commission, Best Practices on the Disclosure of Information in Data Rooms, 2 June 2015 consolidated text, https://competition-policy.ec.europa.eu/system/files/2021-01/bp_disclosure_information_data_rooms_en.pdf

[9] UK Competition and Markets Authority, Sports retailers fined almost GBP 5m for breaching CMA order, 14 February 2022, https://www.gov.uk/government/news/sports-retailers-fined-almost-5m-for-breaching-cma-order

[10] European Commission, Illumina/GRAIL merger control proceedings, https://competition-policy.ec.europa.eu/document/download/4a8ebad9-5f50-40a1-8509-16492efe3dfb_en?filename=2024_Illumina_Grail_en.pdf

[11] Court of Justice of the European Union, Judgment in Case C-746/21 P, Altice Group Lux v Commission, 9 November 2023, https://curia.europa.eu/juris/liste.jsf?num=C-746/21%20P

[12] UK Competition and Markets Authority, Financial services sector: suspected anti-competitive practices, case update, 2025, https://www.gov.uk/cma-cases/financial-services-sector-suspected-anti-competitive-practices

[13] UK Competition and Markets Authority, Merger assessment guidelines, https://www.gov.uk/government/publications/merger-assessment-guidelines

[14] European Commission, Merger procedures, https://competition-policy.ec.europa.eu/mergers/procedures_en

[15] US Federal Trade Commission, Negotiating Merger Remedies, https://www.ftc.gov/advice-guidance/competition-guidance/negotiating-merger-remedies

About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and closure.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners, he is Managing Partner and leads the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

He is also an active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.