

Defend the Control Room: Buying OT Cybersecurity Platforms

Acquisition diligence and investment decisions for industrial security businesses

Authored by Chennakeshav Adya

Independent Researcher

October 2026

ABSTRACT

An acquisition of an operational technology cybersecurity platform requires evidence connecting its permitted product behaviour, customer acceptance, support obligations and cash receipts. This paper proposes a deployment evidence record and an acquisition framework using seven primary technical and governance sources. Draft material is distinguished from final guidance.

Three original figures and three tables organise a qualitative readiness sequence, fictional service economics and investment sensitivities. A four-year author illustration assumes USD 6 million of initial purchase and integration expenditure. At an assumed twelve percent discount rate, specified annual project cash produces net present value of USD 1,118,152. Separate acceptance-delay and support-stress cases produce negative USD 811,073 and negative USD 1,422,249. All inputs are fictional; the calculations exclude tax, debt, working capital and terminal value. They provide no enterprise valuation or empirical benchmark.

The recommendation is to approve consideration and follow-on expenditure against a defined deployment perimeter and costed service obligations. Keep contingent expansion separate and review contractual milestones independently. The framework supplies no product certification, validated maturity score, customer-demand finding or prediction of incident losses. Actual transactions require product-specific engineering, financial, legal and customer diligence.

JEL Classification: G31, G34, L86, L94, L95, O33

Keywords: operational technology, cybersecurity, mergers and acquisitions, utility networks, artificial intelligence, product diligence, customer acceptance, software valuation, integration, support economics

1 The acquisition decision

Define the security function the buyer intends to acquire and the customer environment in which it must operate. An investment thesis might concern asset visibility, monitoring, access management or analyst assistance. Each function implies different permissions and installation requirements. The thesis should identify the current product version, customer deliverable and commercial reason for ownership before attaching a purchase price.

Prepare two records at the outset. The first describes accepted installations and the obligations needed to maintain them. The second describes proposed expansion that has yet to pass customer review. Assign separate financial assumptions to those records. A customer demonstration, a signed pilot and a collected recurring payment answer different questions about readiness and commercial value.

This paper proposes a transaction process for investors and industrial buyers examining those questions. Its analytical contribution is a deployment evidence record connecting technical obligations to contractual cash. The record is a proposed diligence instrument. It needs adaptation to the actual product and does not replace specialist security assessment, operational engineering or jurisdiction-specific legal review.

The committee's immediate decision should specify how much consideration and follow-on expenditure it is prepared to approve for the evidenced business. Describe the rights acquired, products supported, customer commitments and integration dependencies. Keep potential new sectors and geographies in a separately costed expansion case. A recommendation becomes reviewable when the committee can trace each material cash assumption to an installation, contract and delivery plan, and can identify what happens if the assumption fails.

2 Public sources and their boundaries

The joint Secure by Demand guidance hosted by Australia's cyber security agency was published in January 2025. It identifies procurement considerations including configuration control, baseline logging, operator autonomy, secure defaults and vulnerability support.[1] This paper uses that context to frame questions for an acquisition review. It asserts no manufacturer's compliance with the guidance.

NIST's final Guide to Operational Technology Security, Revision 3, was published in September 2023. It addresses the performance, reliability and safety requirements of systems interacting with the physical environment. Its publication page links a September 2026 initial public draft of Revision 4.[2] The draft has not been treated as a final standard here.

Joint secure connectivity guidance published in January 2026 describes desirable end states and documented connectivity business cases.[3] The December 2025 joint AI in OT guidance identifies four principles covering understanding, use cases, governance and safety/security practices.[4] These documents provide context for engineering review. They establish no financial return, vendor ranking or universal obligation applicable to the hypothetical target.

NIST's final SSDF Version 1.1 supplies a secure development vocabulary.[5] Its Cybersecurity Framework 2.0 provides high-level outcomes without prescribing their implementation.[6] The AI Risk Management Framework is voluntary; NIST's current overview also identifies revision activity and an April 2026 critical-infrastructure concept note.[7] The proposed valuation and transaction structures below are original analytical proposals. Their numerical inputs are fictional. Their suitability requires independent review of actual evidence.

3 Specify the acquired product perimeter

Create a product inventory with version identifiers and a clear description of each supported function. Identify software supplied by the target, third-party dependencies, appliances, deployment scripts and hosted services. Record which items are included in the sale and which require another party's licence or consent. The buyer needs a reproducible statement of what it can operate after completion.

Define product behaviour using ordinary engineering terms. State whether a component observes traffic, supplies an alert, proposes a response or can cause an operational change. Identify the permissions required for each behaviour. Describe where a human must approve an action and how that approval is recorded. This proposed classification helps the committee understand the intended deployment and does not establish that any particular architecture is safe.

Tie the inventory to customer contracts. A contract may cover an appliance and annual support, while a demonstration includes a hosted analytics feature absent from the purchased configuration. Review those differences explicitly. Record customer-specific modifications and the person responsible for maintaining them. A product roadmap should distinguish generally released functions from experiments, bespoke work and discontinued components.

At the end of this review, the buyer should possess a dated product schedule it can attach to diligence findings and the integration budget. Material changes to that schedule should trigger another review of contracts and costs. Keep customer topology and sensitive technical records within the authorised diligence environment. Commercial presentations need enough detail to establish the investment perimeter without exposing information that the seller has no permission to distribute.

4 Build a deployment evidence record

The proposed deployment evidence record is the smallest useful link between a product claim and a revenue assumption. Give each material installation a stable identifier. Connect it to the customer entity, product version, deployment architecture, acceptance evidence, support obligation and payment history. Include the date of the last material change and the owner of the next review.

Use a consistent evidence hierarchy. Signed acceptance and received payment can support different parts of the commercial case. A lab report supports only its stated configuration and tests. A sales presentation provides a claim requiring corroboration. Preserve unresolved items as unresolved. Avoid completing a record through extrapolation from a different customer or from a newer product release.

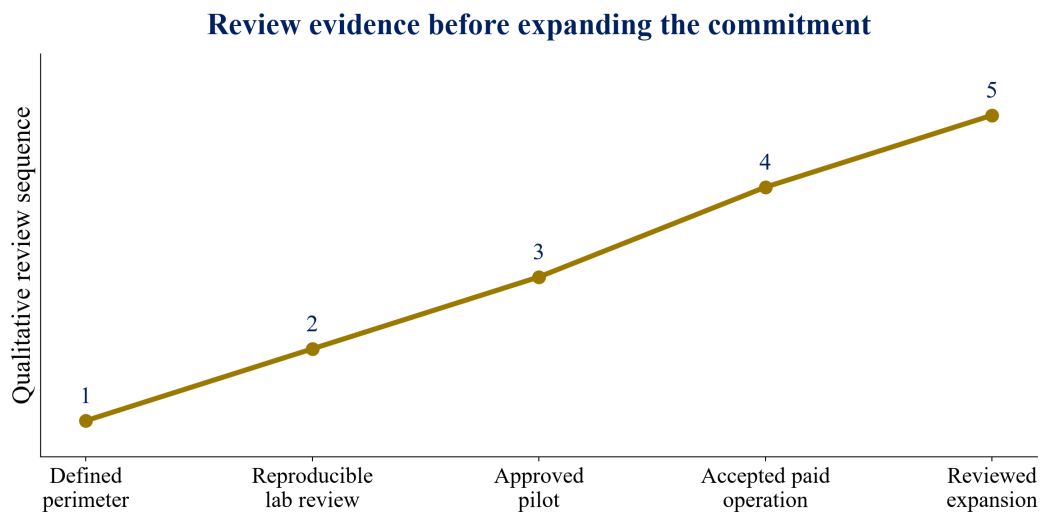
Table 1. Proposed deployment evidence record

Review object	Evidence requested	Investment implication
Product perimeter	Version and function schedule	Assets and obligations acquired
Operational permission	Approved installation and behaviour	Permitted revenue scope
Acceptance	Dated customer decision and exceptions	Timing of contractual receipts
Delivery cost	Support records and resource allocation	Contribution after service costs
Continuity	Recovery rehearsal and dependency register	Integration expenditure and conditions
Commercial rights	Executed contract and consent review	Assignment and renewal assumptions

Table 1 is an author-proposed diligence structure. It contains no observed target data. Complete it using authorised records and name the reviewer responsible for each conclusion. Where evidence is incomplete, identify the cash assumption affected and the action needed before approval. A record that cannot be completed may support a restricted pilot or deferred purchase decision. It supplies no basis for inventing a completion date, a likelihood of acceptance or the commercial value of an installation.

5 Test deployment readiness in sequence

Use a staged review to determine whether further capital should be committed. The proposed sequence begins with a defined product perimeter, proceeds through reproducible lab evaluation and a customer-approved pilot, and reaches paid operation and reviewed expansion. Advancement depends on evidence appropriate to that stage. The sequence is qualitative; its plotted position measures neither security quality nor maturity on a validated scale.

Figure 1. Proposed sequence for reviewing deployment readiness

Author proposal; plotted positions are not validated maturity scores or probabilities.

At the definition stage, require a specific function and intended environment. At the lab stage, require documented tests with their scope and exceptions. Before a pilot, require the operator's permission and an agreed method of supervision. Before including recurring receipts in the acquisition case, examine contractual acceptance, delivery obligations and collection evidence. Expansion requires another review of the new operating perimeter.

Record the reason for every decision to advance or hold. An unresolved dependency may be tolerable in a bounded lab exercise and material to a production purchase. Specify the permitted next activity and the exposure approved for it. Preserve exceptions so a later reviewer can see whether the original limitation has actually been resolved.

The acquisition committee can use this sequence to distinguish existing deployment evidence from funded product development. It should describe the cost and governance of each unfinished stage. Treat the sequence as

a decision aid proposed by the author. It has not been empirically tested, calibrated to transaction outcomes or endorsed by the agencies cited in this paper.

6 Establish architecture and operating permissions

Ask the target to produce a dated architecture record for the exact configurations supporting material customer receipts. Identify collection points, processing locations, external dependencies and the boundaries between customer and supplier responsibility. The review should make the proposed installation understandable to the operator and the buyer's independent engineering team. Resolve material gaps before assuming that the configuration can be replicated.

The joint connectivity guidance provides the context for documenting a connection's purpose, benefit, dependencies and accountable owner.[3] The acquisition review proposed here applies that question to each target installation. Examine whether the customer approved the actual deployed architecture, the hosted services it relies upon and the parties allowed to access it. Review any disagreement between the contract and operational practice.

Assess the proposed post-close architecture separately. A buyer may intend to consolidate hosting, authentication or reporting. Those changes require analysis of their customer permissions, installation effort and commercial consequences. Build a change register naming the intended modification, the approving party and the cost of retaining the existing arrangement while review proceeds.

For acquisition modelling, translate unresolved architecture questions into specific work and timing assumptions. A new customer consent exercise, duplicate environment or migration rehearsal can be costed. The model should show who provides the work and when the expenditure occurs. It should leave the result contingent until evidence supports it. This process makes the financial implication visible without asserting that a redesigned connection is secure or that an operator will permit it.

7 Evaluate the product under authorised conditions

Prepare an evaluation plan with the target and an independent specialist. State the exact configuration, authorised environment, test objectives, prohibited activities and stop conditions. Obtain the operator's approval before any customer-environment activity. This paper proposes diligence questions only; it provides no instructions for intrusive testing or access to an operational system.

A useful review needs enough recorded detail to permit an independent interpretation. Identify the product version, configuration, observation period and reviewer. Preserve the outcome of each agreed check, including failures and incomplete results. The reviewer should explain what the test establishes and the environments to which it cannot be transferred. A summary label such as production ready requires that underlying explanation.

Ask how the product is withdrawn or isolated when its operation falls outside the agreed perimeter. Review the responsibility for pausing use, retaining evidence and notifying the customer. The buyer should understand those obligations before changing support ownership after close. Cost the required staff availability and any customer-specific procedures that the buyer must maintain.

Use evaluation results in the transaction process through explicit dependencies. A satisfactory bounded test may support the next diligence stage. An unresolved operational exception may justify a completion condition or further specialist work. Contractual remedies require legal review and customer agreement where relevant. No proposed test programme can establish universal product safety, the absence of unknown weaknesses or a guaranteed reduction in future incident losses.

8 Review development and product maintenance

Inspect how the target builds and releases the versions used by paying customers. Request version history, approvals, component records, release notes and the documented process for addressing reported weaknesses. Trace a selected resolved issue from report to tested release and customer communication. Agree the sample with the diligence specialist and preserve any limitation in access or completeness.

NIST's SSDF offers a high-level vocabulary for discussing secure software development with suppliers.[5] Use the published framework as context for questions, then examine the target's actual implementation. The paper

proposes an evidence review; it does not score compliance, establish a certification or validate the quality of a development team. The technical reviewer should state what evidence supports each conclusion.

Identify costs that continue after acquisition. These may include dependency maintenance, compatibility work, customer-specific releases and support for older versions. Allocate them to the relevant installations or a clearly described common platform obligation. Avoid assuming that the buyer can immediately discontinue a version that customers are contractually entitled to use.

Build an acquired-product maintenance budget alongside the development roadmap. Name the release capacity required to meet existing commitments before funding additional functions. Describe which planned expenditures maintain current receipts and which enable contingent expansion. This distinction gives the committee a basis for evaluating the timing of investment. It provides no assurance that a planned release can be delivered by a particular date or that customers will accept it.

9 Map dependency and recovery obligations

Prepare a dependency register covering hosted infrastructure, specialist hardware, libraries, model services and personnel needed for material installations. Review supplier contracts and access rights using authorised documents. Establish which dependencies survive a change of control and which require consent, replacement or a new commercial arrangement. The buyer should price the work required to maintain continuity under the reviewed transaction structure.

Ask the target and relevant operator how service can continue during a dependency failure. Review the agreed fallback, retention of essential records and the responsibility for restoration. Examine a documented rehearsal where available and identify its scope. A written plan supplies a proposed procedure; a bounded rehearsal provides evidence about that specific exercise. Neither establishes performance under every operational condition.

Create a cost register for unresolved dependencies. Include duplicate hosting, supplier transition, replacement licences and personnel retention only when their basis is documented or explicitly assumed. State whether a cost occurs before close, during transition or throughout ownership. Keep unsupported quantities open for further review so they do not become hidden assumptions in the price recommendation.

The resulting investment condition should describe an acceptable continuity arrangement and the evidence needed to approve it. Where the arrangement depends on customer permission, the committee must recognise that dependency. Deferred consideration cannot itself provide an operational fallback. Treat negotiated financial protection and engineering continuity as separate workstreams, each with its own owner and approval evidence.

10 Distinguish AI functions and permissions

Describe each AI-enabled function by its input, output and effect on the operator's decisions. Analyst assistance, alert prioritisation and a function that proposes an operational action need separate review. Record whether the model is hosted, locally deployed or supplied by another party. Identify the party responsible for updates and the approvals needed before an altered model reaches a customer installation.

The joint AI in OT guidance provides a governance context encompassing understanding, business-case assessment, assurance and safety/security oversight.[4] The acquisition process proposed here asks the buyer to map those concerns to a specific product and contract. Review the conditions under which a person accepts or rejects a model output and how an operational concern is escalated.

Examine rights to training and evaluation records. Customer permission to process data for a monitoring service requires its own interpretation before another use is assumed. Review the actual contract, restrictions on retention and access to third-party models. Refer ambiguous rights to qualified advisers. This paper gives no legal conclusion about a particular dataset or its transfer in an acquisition.

For the investment model, assign costs to evaluation, model updates, human review and customer approvals. Include a fictional expansion benefit only as an explicitly assumed case. The buyer should identify what additional evidence would support it in an actual transaction. A product labelled AI-enabled provides no independent proof of effectiveness, customer demand, transferable intellectual property or a premium acquisition valuation.

11 Specify evaluation and change governance

Propose an evaluation record for each material model or rule change. Name the intended function, evaluation data, reviewer and acceptance conditions. Describe the limitations of the available data and the circumstances requiring another review. Preserve the prior approved configuration and a documented route for withdrawing the proposed change. The operator should decide which changes require its own approval.

NIST's AI Risk Management Framework is voluntary and addresses trustworthiness considerations across AI development and use.[7] Its existence supplies a reference for governance discussions. It does not validate a target's model or establish a transaction-specific legal obligation. The buyer's assessment needs direct evidence from the products, customers and engineering reviews involved.

Require a clear separation between technical evaluation and commercial release authority. A development team may consider a change ready for a controlled trial while the customer still requires another review. Record both decisions. Cost the continued support of the existing configuration during that interval. Include the responsibility for explaining model changes to operators and documenting any customer-specific restrictions.

Make the change register part of the post-close reporting package. Report proposed changes, completed reviews, unresolved exceptions and expenditure against the approved budget. Relate material exceptions to the affected receipts and service commitments. The objective is to give the buyer a reviewable decision history. The proposed governance process has not been validated as a method of reducing incident frequency or increasing investment returns.

12 Reconcile revenue to accepted installations

Start financial diligence with contracts and collected cash. Reconcile the customer ledger to invoices, acceptance documents, service periods and receipts. Identify pilot fees, implementation payments, hardware sales, subscriptions and support separately. Describe the basis on which each item is included in a cash forecast. An invoice under review and an accepted recurring service require different collection assumptions.

Trace a sample of material revenue cohorts to the deployment evidence record. Examine whether the product configuration that generated the invoice remains supported. Review unresolved customer exceptions and any contracted right to withhold payment, obtain a credit or terminate. The financial reviewer should document the limitations of its access and the assumptions needing legal interpretation.

Evaluate expansion proposals at the level of the actual contract. A multi-site customer may have authorised one installation and retained discretion over the rest. Proposed expansion needs its own acceptance process, staffing and collection timetable. Avoid treating every site mentioned in a commercial discussion as committed revenue. Record a conditional expansion case separately from existing contractual receipts.

The acquisition model should reflect the reviewed payment schedule and cost of delivering the promised service. Where a customer reference cannot be obtained, preserve that absence in the diligence report. It may affect the scope of the committee's approval or the work required before close. This paper identifies no observed revenue quality, renewal rate or willingness to pay for a particular platform.

13 Calculate installation and support economics

Define the unit of service before comparing its economics. A site, asset, appliance, monitored connection or analyst seat can represent a different obligation. Specify the contracted unit and the installation boundary. Allocate implementation and continuing support costs through a consistent method. Document the treatment of common development expenditure so the committee can reproduce the contribution calculation.

Separate initial work from annual costs. Initial work might include permitted configuration, customer training and acceptance review. Continuing costs might include hosting, software maintenance and contracted support. Record which costs are included in the price and which are borne by the operator. Review those allocations against signed terms instead of inferring them from the sales description.

Examine how support changes with the deployment mix. A proposed new geography or product behaviour may require additional engineers, permissions and customer review. Price that work explicitly in a scenario. The existing contribution at one deployment type supplies no observed benchmark for a different type. An investment committee should ask what direct evidence supports a claimed saving or increased service capacity.

Use a cost register with named assumptions and source dates. Where actual staff records or supplier terms are unavailable, mark the input as an assumption in ordinary prose and test its financial effect. The contribution measure should identify costs it excludes. The next section illustrates a reproducible comparison using fictional data; it describes no target company, measured product performance or available vendor quotation.

14 Compare cost and defined acceptance evidence

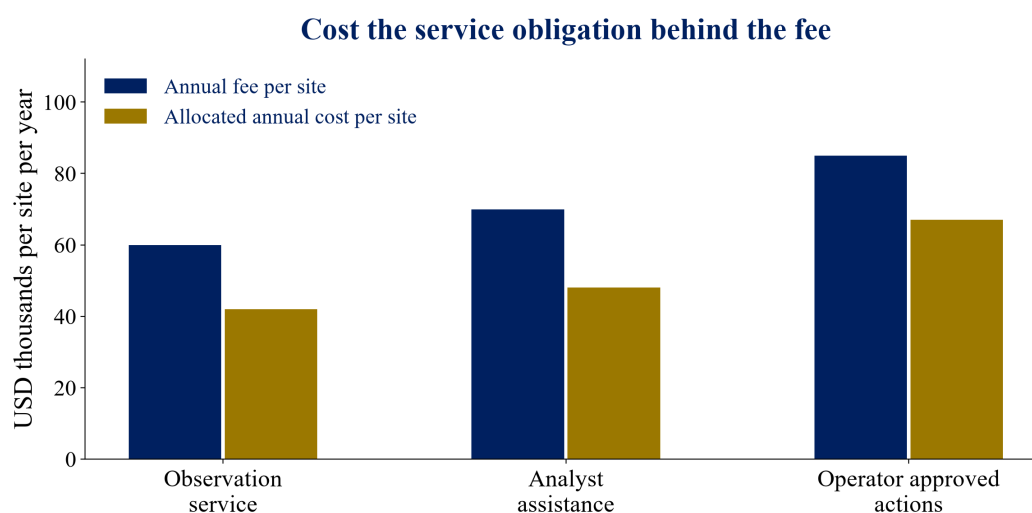
The following fictional comparison assumes fifty sites in each configuration and twenty agreed acceptance checks per site. The checks are assumed to be completed solely to demonstrate a calculation. Their identical count provides no equivalence in actual security performance. Every fee, cost and check count is an author assumption. The three configurations describe possible service scopes rather than named products.

Table 2. Fictional annual service economics in USD thousands

Assumed configuration	Fee per site	Variable cost per site	Common cost	Annual contribution
Observation service	60	30	600	900
Analyst assistance	70	32	800	1100
Operator approved actions	85	45	1100	900

For the observation service, fifty assumed fees of USD 60,000 generate USD 3 million. Variable delivery expenditure of USD 1.5 million and common costs of USD 600,000 leave USD 900,000. The other rows follow the same arithmetic. Contribution excludes initial implementation, tax, financing and working-capital effects. It is an annual model output and establishes no actual margin.

Figure 2. Fictional fees and allocated delivery costs per site



Fictional 50-site cases; no observed cost, fee or cybersecurity performance benchmark.

Allocated annual costs per site are USD 42,000, USD 48,000 and USD 67,000. Dividing those amounts by twenty assumed checks produces USD 2,100, USD 2,400 and USD 3,350 per agreed check. That ratio is a proposed costing view, not a cybersecurity effectiveness score. An actual comparison requires equivalent conditions, independently reviewed results and a defined service obligation. The table shows why the acquisition model should identify both the price of a service and the work needed to supply it.

15 Frame a limited acquisition cash model

Use a limited financial illustration to expose the decision dependencies. The base case assumes USD 5 million of purchase consideration and USD 1 million of initial integration expenditure, both paid at time zero. It assumes year-end project cash of USD 1.8 million, USD 2.2 million, USD 2.6 million and USD 3 million. The discount rate is an assumed twelve percent annually.

Discount each annual amount to time zero and subtract the USD 6 million initial outlay. The resulting four-year net present value is USD 1,118,152, rounded to the nearest dollar. The sum of the discounted operating cash is

USD 7,118,152. These are arithmetic results from fictional inputs. They identify neither a market enterprise value nor an appropriate transaction price.

The model deliberately ends after four years and assigns zero terminal value. It excludes corporate tax, debt, working capital, transaction expenses beyond the assumed integration sum and proceeds from a later sale. Real acquisitions need those items reviewed separately. The illustration also provides no probability-weighted forecast. The assumed cash amounts must not be interpreted as management estimates from a real business.

The committee can use this calculation structure to understand which evidence would support an actual investment model. Customer acceptance determines the timing of some receipts, support commitments affect costs and consent requirements can affect both. Populate the real model using authorised transaction evidence and explain every residual assumption. Any committee return threshold and financing requirement must be established by the actual buyer.

16 Examine delay and support sensitivities

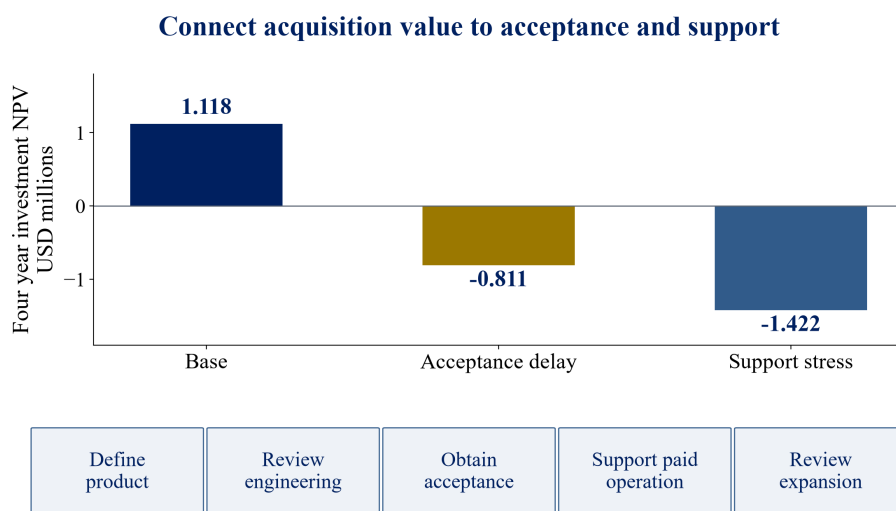
The fictional acceptance-delay case retains the USD 6 million initial outlay and substitutes annual project cash of USD 600,000, USD 1.8 million, USD 2.2 million and USD 2.6 million. At the same discount rate and four-year horizon, its net present value is negative USD 811,073. This case assumes a particular receipt and cost pattern; it provides no estimated probability of customer delay.

The fictional support-stress case increases the initial outlay to USD 6.5 million and assumes annual project cash of USD 1.4 million, USD 1.6 million, USD 1.8 million and USD 2 million. Its net present value is negative USD 1,422,249. The additional initial expenditure and lower cash amounts are assumed solely for this illustration.

Table 3. Fictional four year investment sensitivities in USD millions

Case	Initial outlay	Cash years one to four	Net present value
Base	6.0	1.8; 2.2; 2.6; 3.0	1.118
Acceptance delay	6.0	0.6; 1.8; 2.2; 2.6	-0.811
Support stress	6.5	1.4; 1.6; 1.8; 2.0	-1.422

Figure 3. Fictional acquisition sensitivity and proposed commercialisation sequence



Fictional 4-year cash cases; 12% discount; no tax, debt, working capital or terminal value.

The discounted-value differences describe the financial consequences of the specified assumptions. They support requests for evidence about acceptance timing and support costs. They establish no causal estimate of how diligence, contractual protection or technical changes affect returns. An actual investment committee should select sensitivities relevant to its target and document the basis for their inputs. Keep mitigation expenditure within the model when a proposed remedy requires additional work.

17 Design consideration around reviewable obligations

Develop a purchase structure only after defining the acquired assets and continuing obligations. Fixed consideration, retained amounts, deferred payments and contingent consideration each require legal, tax and accounting review. The author proposes matching any conditional payment to a milestone whose evidence is understandable to both parties and capable of independent review.

An acceptance-related milestone should specify the customer entity, contracted configuration, acceptance document and treatment of exceptions. A collections milestone needs an agreed receipt definition and rules for credits, offsets and disputed invoices. Where the buyer controls delivery after close, the parties should examine how that control affects the seller's opportunity to satisfy the condition.

Avoid using a generic security maturity score as a payment trigger without a defined assessment method. The readiness sequence in this paper is qualitative and supplies no validated score. A reviewer could verify completion of an agreed test or delivery of a contractual record within its scope. The parties must still resolve how disputes, delayed permissions and changes in the service perimeter are treated.

Cost the continuing obligation alongside any deferred payment. A retained purchase amount supplies financial protection subject to its terms and enforceability. It does not provide an engineer, customer permission or operational continuity. Allocate those responsibilities explicitly. The proposed consideration approach offers a negotiation framework; it establishes no observed market practice, recommended proportion of the price or enforceable remedy in a particular jurisdiction.

18 Review geographic and sector expansion

Assess expansion through the deployment conditions in the proposed geography and sector. A water operator, electricity network and industrial manufacturer may have different contracts, approval routes and service requirements. Identify the actual buyer, contracting authority and installation environment. Use qualified local advisers to assess applicable rules and procurement conditions. The paper assumes no common regulatory regime across them.

Prepare a separate expansion budget. Include product adaptation, customer review, support availability, authorised hosting and sales costs where their basis can be established. State whether the target already possesses the relevant rights and resources. Treat an untested sector application as proposed development with its own evidence requirements. Avoid inheriting acceptance conclusions from an unrelated deployment.

Evaluate channels and partners by their contractual contribution. A distributor agreement might permit introductions, installation or support under different terms. Review who bears the service obligation and who receives customer cash. Identify termination and change-of-control conditions before assigning channel receipts to the acquired business. No partner relationship should enter the model through an unsupported description of its reach.

The committee's expansion case should state the initial bounded activity it is funding and the conditions for further commitment. It could authorise a locally reviewed pilot while retaining a separate decision on broader deployment. This paper makes no claim about demand in the UK, US, India or GCC, and offers no geographic ranking. Expansion value remains contingent on customer, technical and contractual evidence.

19 Budget the commercialisation sequence

Translate the readiness sequence into a funded work programme. Define the product and contract perimeter, complete the required engineering review, obtain customer acceptance, maintain paid operation and review expansion. The order reflects dependencies in the proposed acquisition process. It sets no universal calendar and estimates no elapsed time for regulatory, technical or customer approval.

For each activity, assign an accountable owner, deliverable and resource budget. Describe the evidence permitting the next commitment. A lab evaluation might require a specialist report; an installation might require an operator's signed permission and accepted configuration. Keep continuing support funded while new work is reviewed. The committee should understand the cost of preserving the existing service throughout the sequence.

Separate expenditure required for continuity from expenditure intended to create new receipts. The former supports obligations already assumed by the buyer. The latter requires a defined commercial hypothesis and

evidence plan. State the maximum approved exposure and the decision required to expand it. Review any delay against the cash forecast and service commitments affected.

The roadmap in Figure 3 is an author proposal summarising these dependencies. It contains no validated dates, probability of success or evidence that the fictional target can complete them. Its practical use is to make responsibilities and approval requirements visible. An actual roadmap should be agreed with the target, operators and transaction advisers, then revised when product behaviour, customer conditions or available resources change.

20 Plan ownership and integration at completion

Prepare a completion plan that preserves existing customer obligations while changing ownership. Identify the staff, access rights, supplier relationships and records needed on the first day. Review any transfer restriction or customer consent requirement. Document the permitted access of the buyer's team and protect customer information through the approved transaction process.

Set responsibility for each supported product version. Name the team that answers customer questions, manages agreed updates and escalates operational concerns. Include contractual response commitments in the staffing plan. Inspect the workload and available capacity using authorised records. Treat any forecast of increased capacity as an assumption until a resourced plan supports it.

Evaluate platform consolidation through a separate approved change programme. A commercial desire to combine systems should be translated into specific modifications, customer approvals, testing and expenditure. Maintain the existing configuration when the approved plan requires it. The acquisition case should carry the cost of parallel operation and the resources needed to review the change.

Establish reporting appropriate to the continuing service. Include material customer exceptions, overdue collections, support workload and unresolved integration dependencies. The proposed report helps the owner review its commitments and expenditure. It does not establish that a consolidated architecture will perform better or that ownership change creates a financial synergy. Recognise a claimed synergy only through a clearly described and evidenced operating change.

21 Set financing against evidenced cash

Prepare a funding plan that distinguishes purchase consideration, initial integration, continuing support and contingent expansion. Identify the source and timing of each payment. Reconcile the plan to contractual receipts and the proposed operating budget. An acquisition funded with equity still needs enough liquidity to maintain the obligations that accompany ownership.

If debt is contemplated, obtain actual terms and assess the financing against the reviewed cash forecast. Examine the treatment of delayed acceptance, restricted receipts and integration expenditure under the proposed documents. Consult relevant advisers about security, covenants and customer-contract constraints. This paper supplies no lender quote, borrowing capacity or assumption that a software acquisition qualifies for project finance.

Use the adverse cases to identify a possible liquidity requirement, then model it explicitly. A negative net present value is a discounted investment result. It does not by itself specify when cash runs out. A separate period-by-period cash schedule needs financing flows, tax, working capital and payment dates before drawing that conclusion. The limited four-year illustration omits those items.

The proposed financing decision should describe the available funds, conditions for drawing them and continuing reserves approved by the buyer. Keep future refinancing and sale proceeds outside the base case until their assumptions are stated and reviewed. The recommendation remains contingent on actual financial records and negotiated terms. No structure in this paper guarantees financing availability, repayment or preservation of invested capital.

22 Assemble the investment committee record

Build a concise decision record that links the proposed acquisition to its evidence. Include the product perimeter, installation records, customer cash reconciliation, support budget and material contractual dependencies. Attach specialist conclusions with their limitations. The committee should be able to identify which findings support the recommended commitment and which assumptions remain open.

State a proposed approval condition for each material unresolved item. Describe the evidence required, reviewer and expenditure permitted before resolution. Conditions should be sufficiently specific to review at completion. Avoid substituting a broad statement of satisfactory diligence for a defined deliverable when the uncertainty affects a material revenue or continuity assumption.

Use the high-level risk outcomes in NIST's Cybersecurity Framework as a reference for discussions with the responsible specialists.[6] The author proposes a transaction-specific decision record built from direct evidence. A mapping to an outcome supplies an organising label. It does not establish that the platform achieves the outcome, passes an audit or meets a customer obligation.

The final recommendation should report the price and follow-on budget for the evidenced case, the consequences of the stated adverse cases and the proposed next decision. Document dissent and matters outside the review scope. A committee may approve, defer, restrict or decline a transaction. This framework provides no preferred result before the underlying evidence is assessed and no assurance of a successful investment after approval.

23 Research limitations and further testing

The paper is a source-grounded conceptual framework with fictional financial illustrations. It contains no dataset of acquisitions, product tests or utility purchasing decisions. It therefore estimates no relationship between deployment diligence and transaction performance. All readiness positions, fees, cost allocations and cash amounts are author proposals or assumptions. Their purpose is to make a decision method reproducible.

The public sources supply different technical and governance contexts. They have not been treated as a common certification or a complete statement of applicable law. Draft and concept-note material is identified by status. Product-specific engineering, privacy, intellectual-property, procurement and transaction questions require appropriately qualified review. The paper makes no conclusion about the enforceability of proposed terms.

Further research could examine whether the deployment evidence record can be completed consistently across consenting transactions. A study would need a defined sample, authorised access, a coding method and protections for operational information. It should distinguish missing evidence from a failed product or a failed investment. Publication would require a lawful basis for sharing the resulting records.

An empirical financial study would also need a clear definition of return, ownership period, tax treatment and capital invested. It should account for development expenditure and service obligations after close. Those data are absent here. Readers should use the proposed instruments as questions for actual diligence and replace the fictional inputs before making any product, acquisition or financing decision.

24 Conclusion and the next decision

Approve an OT-security acquisition against the functions, installations and obligations the buyer can substantiate. The proposed deployment evidence record connects a product version and approved operating perimeter to acceptance, support costs and customer cash. It allows the investment committee to locate an uncertainty and identify the work required to resolve it.

The fictional comparisons illustrate two financial questions. Annual service contribution depends on the cost of supplying the promised configuration. The acquisition result depends on the timing and level of project cash and initial expenditure. The calculations show those consequences under stated assumptions. They establish no market benchmark, vendor superiority or likelihood of earning the modelled return.

Before further commitment, obtain the records supporting material installations and ask independent specialists to review their scope. Reconcile receipts to the relevant service obligations. Cost the continuity plan, unresolved permissions and proposed integration. Review any deferred consideration against milestones that both parties can evidence. Maintain a separate, conditional expansion case for new behaviours, sectors and geographies.

The recommended next step is a bounded acquisition assessment with an agreed evidence request and named reviewers. Its output should state the acquisition perimeter, support obligations, financial assumptions and conditions requiring resolution. That assessment gives the buyer a basis for deciding whether to proceed and how much further capital to commit. Actual results remain dependent on the target's evidence, customer decisions and negotiated transaction terms.

Frequently Asked Questions

What should a buyer establish before pricing an OT security platform?

Define the product versions and functions being acquired, then connect material installations to customer permissions, acceptance, support costs and collected cash. This paper proposes a deployment evidence record for that review. Specialist technical, financial and legal assessment remains necessary for the actual transaction.

Does a successful demonstration establish production readiness?

A demonstration provides evidence only about its stated environment and configuration. Production review requires the actual operator's permissions, agreed evaluation and customer acceptance. The qualitative readiness sequence is an author proposal and provides no validated maturity score or prediction of product safety.

How should AI enabled features enter acquisition diligence?

Identify their inputs, outputs, operational effect and approval requirements. Review model changes, evaluation evidence, customer data rights and continuing human oversight. Include the associated resources in the investment case. An AI label establishes no measured effectiveness, customer demand or valuation premium.

Are the service cost figures observed industry benchmarks?

Every fee, site count, delivery cost and acceptance-check count in the comparison is fictional. The figures demonstrate cost allocation and contribution arithmetic. The cost per assumed check is a proposed costing measure and supplies no comparison of cybersecurity effectiveness.

Is the four year calculation an enterprise valuation?

It is a limited acquisition investment illustration with fictional purchase and integration costs. It excludes tax, debt, working capital and terminal value. Its net present value describes the specified cash flows and supplies no transaction price, market enterprise value or probability-weighted forecast.

Can deferred consideration resolve an operational dependency?

A negotiated payment condition addresses financial rights subject to its terms and legal review. The buyer still needs the people, permissions and continuity arrangements required to supply the service. The proposed diligence treats financial protection and operational delivery as separate responsibilities.

Can the same deployment evidence support expansion into another geography?

Review the actual new operator, contract, installation perimeter and applicable requirements. Existing evidence supports only its documented conditions. The expansion case should fund the additional review, support and permissions needed. This paper provides no geographic demand ranking or universal regulatory conclusion.

What is the recommended next transaction step?

Commission a bounded acquisition assessment with a defined evidence request and named independent reviewers. Reconcile the product perimeter, material installations, customer cash and support budget. Report unresolved dependencies and the conditions for further commitment before recommending a purchase structure or funding plan.

References

1. Australian Signals Directorate Australian Cyber Security Centre and partner agencies. Secure by Demand. Published 14 January 2025. <https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/secure-by-demand> . Accessed 4 October 2026.
2. NIST. Guide to Operational Technology Security, SP 800-82 Revision 3. Final September 2023; publication-page note links initial public draft Revision 4 dated September 2026. <https://csrc.nist.gov/pubs/sp/800/82/r3/final> . Accessed 4 October 2026.
3. Australian Cyber Security Centre and partner agencies. Secure connectivity principles for Operational Technology. Published 15 January 2026. <https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/secure-connectivity-principles-for-operational-technology> . Accessed 4 October 2026.
4. New Zealand National Cyber Security Centre and partner agencies. Principles for the Secure Integration of Artificial Intelligence in Operational Technology. Published 3 December 2025. <https://www.ncsc.govt.nz/protect-your-organisation/principles-for-the-secure-integration-of-ai-in-ot/> . Accessed 4 October 2026.
5. NIST. Secure Software Development Framework Version 1.1, SP 800-218. Final February 2022. <https://csrc.nist.gov/pubs/sp/800/218/final> . Accessed 4 October 2026.
6. NIST. The NIST Cybersecurity Framework 2.0, CSWP 29. Published 26 February 2024. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> . Accessed 4 October 2026.
7. NIST. AI Risk Management Framework overview. Identifies voluntary AI RMF 1.0, current revision activity and April 2026 critical-infrastructure concept note. <https://www.nist.gov/itl/ai-risk-management-framework> . Accessed 4 October 2026.

About the Author

Authored by Chennakeshav Adya Independent Researcher

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 close.

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, leading 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.

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.