

Cyber Risk at the Pump: Pricing OT Exposure in Water Utilities

A diligence, valuation and capital-allocation framework for cyber-physical utility risk

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Background. Water utilities depend on operational technology to monitor and control abstraction, treatment, pumping, dosing, storage and distribution. Connectivity, remote access, cloud services and integrated data can improve performance while creating paths through which a cyber incident can affect physical service. A generic cyber score does not show how exposure changes enterprise value, debt capacity, concession compliance or capital need. Objective. This paper develops a framework for translating water-sector operational-technology exposure into investment and transaction decisions. Method. It synthesises current NIST, EPA, CISA, FBI, United Kingdom regulatory and securities-disclosure guidance. It then maps critical services, cyber-physical scenarios, control evidence, recovery capability and contractual allocation into cash-flow pathways, remediation capital, valuation cases, financing protections and implementation gates. Findings. Cyber exposure should be priced through defined mechanisms: unsafe or unavailable process control, service interruption, emergency operation, restoration cost, regulatory action, customer remedy, delayed capital delivery, third-party failure, disclosure and financing effects. Control maturity changes scenario likelihood, duration, detection and recovery; it does not justify a universal percentage discount. Implications. Buyers, lenders, boards and public authorities can make stronger decisions when technical diligence identifies the systems and dependencies that sustain essential service, tests safe fallback and recovery, and links each material gap to an accountable action, cost, timetable and transaction response. All unattributed numerical exhibits are hypothetical decision tools; they are not forecasts, valuations, offers or descriptions of a named utility or transaction.

JEL Classification: G31, G32, G34, L95, O33, Q25

Keywords: water utility, operational technology, cybersecurity, SCADA, valuation, due diligence, project finance, public-private partnership, resilience, capital allocation

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. THE PRICING QUESTION

The investment question is not whether a water utility has cyber risk. It is how a specific weakness could interrupt or corrupt an essential service, how long the consequence could persist, what cash and capital pathways would follow, and which party would bear them. Pricing begins with the physical process and contractual perimeter.

A buyer, lender or public authority should define the transaction, service obligations, protected assets, financing structure, regulatory regime, incident history, control evidence and decision threshold before assigning economic consequences.

2. OT IS CYBER-PHYSICAL

Operational technology observes and changes physical processes. In water systems it can control pumps, valves, chemical dosing, tank levels, treatment sequences, pressure and protective shutdowns. NIST defines OT around programmable systems that interact with the physical environment and emphasises performance, reliability and safety requirements [1].

This distinction matters because confidentiality, integrity and availability can produce physical consequences. A control decision that is acceptable for office systems may be unsafe for a treatment or distribution process.

3. ESSENTIAL SERVICE FIRST

The analysis should start with essential service: safe water, required pressure, reliable wastewater collection, compliant discharge and timely recovery. Technology assets matter through their role in those outcomes. The United Kingdom classifies drinking-water supply and distribution as an essential service under the NIS regime [2].

The diligence team should identify the minimum service that must continue, the processes that sustain it and the time available before an interruption becomes material.

4. A RISK SCORE IS NOT A PRICE

A maturity score can support prioritisation, yet it rarely reveals the cash effect of an incident. Two utilities with similar scores can have different network architectures, manual capability, customer exposure, regulatory obligations and recovery times. A numerical rating can also create false precision where evidence is incomplete.

The valuation process should retain the underlying gap, affected process, credible scenario, control dependency, recovery evidence and financial mechanism.

5. THE CYBER-TO-VALUE CHAIN

The core chain connects threat, exposure, control failure, process effect, service consequence, response, contractual or regulatory consequence and cash flow. Each link should be supported or identified as a management assumption. Breaking one link can materially reduce exposure.

For example, insecure remote access may create a path, network segmentation may limit movement, independent process protection may prevent unsafe dosing, and tested manual operation may reduce outage duration.

6. SYSTEM MAP

The system map should show enterprise IT, supervisory control, engineering workstations, historians, remote-access services, programmable controllers, field devices, safety or quality

protections, telecommunications, cloud dependencies and third parties. Trust boundaries and data flows matter more than a flat asset list.

NIST SP 1800-45 provides three reference designs for secure remote access in water and wastewater environments using commercially available technologies [3]. The designs support architecture analysis; they do not certify a specific utility.

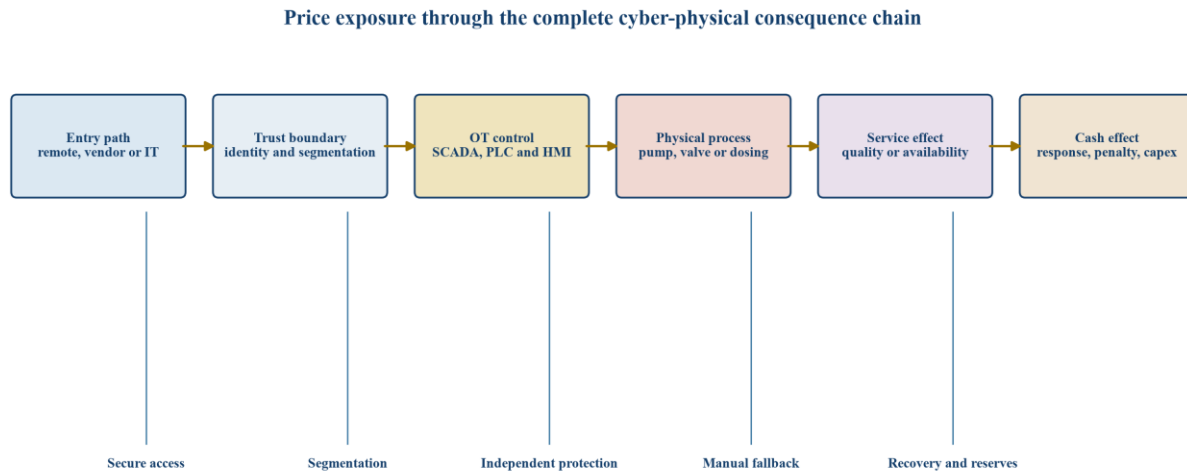


Figure 1. From cyber entry path to water-service and financial consequence

Generic architecture; actual zones, controls, service obligations and financial consequences depend on the utility and jurisdiction.

7. ASSET INVENTORY

The inventory should identify devices, software, firmware, owners, locations, functions, communication paths, support status and criticality. CISA, EPA and FBI include OT and IT inventory among their top actions for water systems [4]. Unknown assets can remain unpatched, externally exposed or absent from recovery plans.

Inventory accuracy should be tested against network discovery, field inspection, procurement and maintenance records. Active discovery in sensitive OT needs engineering approval.

8. CROWN-JEWEL SERVICES

Crown jewels are the functions whose compromise could create intolerable service, safety, environmental or financial consequences. They can include dosing control, source switching, high-lift pumping, reservoir control, laboratory results, alarm management, engineering configuration and communications.

The utility should identify the minimum systems, people, facilities and supplies required to sustain each service. A server can be replaceable while the configuration, credentials or specialist knowledge around it are not.

9. ARCHITECTURE ZONES

Segmentation limits pathways between corporate IT, supervisory systems, control zones, safety functions and external services. Architecture diagrams should reflect current implementation and permitted flows. A firewall shown on a diagram is weak evidence without configuration, rule review, logging and test results.

The diligence team should examine temporary connections, vendor tunnels, wireless links, cellular modems, dual-homed hosts and maintenance laptops that can bypass intended boundaries.

10. REMOTE ACCESS

Remote access supports operations and specialist maintenance while creating a material entry path. Controls can include named identity, multifactor authentication, managed devices, approval, session recording, time limits, least privilege, monitored jump services and rapid revocation.

The review should test actual access rather than policy alone. Dormant accounts, shared credentials and supplier-managed gateways can outlive the service need that created them.

11. INTERNET EXPOSURE

Public-facing OT devices, management interfaces and weakly protected remote services can expose control environments. CISA's water-sector guidance directs operators to reduce public internet exposure and address insecurely connected OT [4]-[5].

Exposure testing should be authorised and coordinated with operations. The capital plan should include secure alternatives, field work and downtime where remediation cannot be completed through configuration.

12. IDENTITY AND PRIVILEGE

Privileged access can change logic, disable alarms, alter setpoints or interrupt service. Controls should separate administrative, engineering and operating roles; use individual accounts; protect credentials; and review entitlements.

Emergency access needs a controlled process that remains available during communications failure. The utility should demonstrate revocation for departed staff and suppliers.

13. DEFAULT CREDENTIALS

Default or weak credentials remain material in embedded devices and older control systems. The CISA advisory concerning exploitation of programmable controllers at water and wastewater facilities highlights default or absent passwords and insecure internet connection [5].

Remediation should include supported credential change, network restriction, configuration backup and safe testing. Replacement may be required where a device cannot support adequate control.

14. ENGINEERING WORKSTATIONS

Engineering workstations can modify controller logic and configurations. Their compromise can have a greater physical consequence than a typical user device. They should be hardened, access controlled, monitored, backed up and separated from general browsing and email.

Diligence should identify portable tools, contractor laptops and offline media used for maintenance. A protected central workstation does not address unmanaged field pathways.

15. PLC AND HMI INTEGRITY

Programmable logic controllers and human-machine interfaces implement and display control. Integrity measures can include approved logic baselines, change detection, access restrictions, signed or verified updates where supported, and comparison against known-good configuration.

The investment case should distinguish compensating controls for legacy devices from a funded replacement plan. Unsupported equipment can create accumulating operational and cyber debt.

16. INDEPENDENT PROTECTION

Safety and quality should not depend solely on the same control path that can be compromised. Independent interlocks, physical limits, laboratory confirmation, local indication and operating procedures can reduce consequence.

The diligence team should verify independence in design and practice. Logical separation within one vulnerable platform may not provide the assumed protection.

17. MONITORING

Monitoring should collect events that reveal unauthorised access, configuration change, abnormal communication and process anomaly without compromising system performance. Coverage should be mapped to crown-jewel services.

Alert volume alone is not evidence of detection. The team should test whether responsible staff receive, interpret and escalate a relevant event within the required time.

18. TIME AND LOGGING

Investigation and recovery depend on accurate time, retained logs and protected evidence. OT devices can have limited storage or inconsistent clock configuration. Central collection should account for intermittent connectivity and device constraints.

Retention should reflect regulatory, operational, insurance and transaction needs. Sensitive logs should be access controlled because they can reveal architecture and weaknesses.

19. VULNERABILITY MANAGEMENT

Vulnerability management includes identification, applicability, operational consequence, mitigation, testing and closure. Patch speed cannot be copied directly from enterprise IT where shutdown or vendor certification is required.

The utility should show risk-based scheduling, compensating controls and documented acceptance. A long backlog needs separation between irrelevant software findings and vulnerabilities with credible control-system pathways.

20. SECURE CONFIGURATION

Configuration baselines should cover operating systems, network devices, controllers, remote access, cloud services and applications. Deviations should be approved and periodically reviewed. Configuration drift can reintroduce exposure after a remediation programme.

Evidence can include baseline records, automated checks where safe, change tickets and sampled devices. Policy statements without device evidence provide limited transaction assurance.

21. BACKUP

Backups should cover data, configurations, controller logic, virtual systems, licences, keys and documentation. NIST published an OT Backup Quick Start Guide in 2026, reinforcing the need to address the distinct recovery requirements of operational environments [6].

Backup success should be separated from restoration success. Offline or protected copies, integrity checks and tested rebuild sequences matter when production systems and connected repositories are compromised together.

22. RECOVERY

Recovery planning should identify the sequence, dependencies, authority, facilities, communications and time needed to restore essential service. The sequence may prioritise process visibility, safe local control and selected zones before enterprise integration.

Recovery time should be demonstrated through exercises and technical tests. An assumed target without available hardware, configuration, specialist access and field procedures should remain a management estimate.

23. MANUAL OPERATION

Manual operation can reduce consequence when automation is unavailable, subject to staffing, access, safety and duration. Procedures should identify which services can operate manually, required skill, local indications, communications and supply constraints.

The review should test realistic conditions, including night shifts and simultaneous incidents. A written procedure can fail where valves are inaccessible or experienced operators are unavailable.

24. INCIDENT RESPONSE

The plan should align executive, operational, technical, legal, regulatory, communications and law-enforcement actions. The joint CISA, EPA and FBI guide describes sector-specific coordination and the information responders may need, including IT and OT network layouts [7].

Decision rights should cover isolation, manual transition, public notification, evidence preservation, service restoration and materiality assessment.

25. EXERCISES

Tabletop exercises test roles and decisions; technical exercises test tools and restoration; field exercises test physical service. Scenarios should include compromised credentials, lost visibility, altered logic, ransomware, supplier failure and communications outage.

Actions should be assigned, funded and closed. Repeating an exercise without correcting known gaps can create misleading assurance.

26. SUPPLIER ACCESS

Integrators, equipment vendors, managed service providers and software suppliers can hold privileged access or critical knowledge. Contracts should identify access, subcontractors, security obligations, notification, evidence, support, exit and liability.

The utility should retain the ability to revoke access and operate during supplier unavailability. Transaction diligence should identify informal arrangements that are not reflected in contracts.

27. CLOUD DEPENDENCY

Cloud services can host analytics, identity, remote access, monitoring, work management or data exchange. The architecture should identify what happens when the service, internet path or identity provider is unavailable.

Shared responsibility should be specific. Recovery, data portability, jurisdiction and concentration should enter the risk and valuation analysis.

28. TELECOMMUNICATIONS

Control sites can depend on leased lines, radio, cellular or satellite services. Cyber and physical failures can affect the same route or provider. The utility should understand coverage, failover, power and restoration priority.

Redundancy should be tested for common dependencies. Two commercial links can terminate in the same exchange or rely on the same power supply.

29. PHYSICAL SECURITY

Field cabinets, pumping stations, antennas, ports and engineering equipment can provide physical paths into OT. Cyber diligence should connect with site security, visitor control, keys, tamper evidence and environmental protection.

Remote sites require a proportionate model that balances access for safe maintenance with prevention and detection.

30. WORKFORCE

Operators, engineers and technicians understand the process and its safe states. Cyber programmes should use that knowledge and provide role-specific training. Generic awareness alone does not teach an operator how to respond to a suspicious setpoint or lost telemetry.

Succession, contractor dependence and on-call coverage affect recovery. The capital plan may require people and procedures as well as technology.

31. THREAT, VULNERABILITY AND CONSEQUENCE

A threat is a potential cause of harm; a vulnerability is a weakness; consequence is the result if a scenario succeeds. Combining them into one label can obscure remediation. Removing a pathway can reduce likelihood; independent protection can reduce consequence; recovery can reduce duration.

The financial model should show which control changes which part of the scenario.

32. SCENARIO LIBRARY

Useful scenarios are specific enough to test. Examples include unauthorised remote access to a pumping station, compromise of an engineering workstation, alteration of dosing logic, ransomware affecting supervisory visibility, manipulated level data, loss of a cloud identity service and malicious supplier access.

Each scenario should state initiating conditions, affected systems, physical effect, detection, containment, fallback, recovery and financial mechanisms.

33. SERVICE INTERRUPTION

An incident can reduce production, pumping, pressure, storage control or wastewater collection. Financial consequences can include emergency operations, alternative supply, overtime, contractor cost, customer remedy, lost availability payment or regulatory action.

Duration is often more important than the initial technical event. Recovery evidence should therefore influence downside cases and reserves.

34. WATER-QUALITY CONSEQUENCE

Corrupted monitoring, alarms or dosing control can create concern about water quality and require precautionary action even when harmful water is not confirmed. Sampling, flushing, alternative supply, communication and regulatory engagement can create cost.

The model should distinguish a control-system compromise, a confirmed process deviation and a verified quality event. Unsupported assumptions about health impact should not enter valuation as fact.

35. WASTEWATER CONSEQUENCE

Wastewater incidents can affect pumping, treatment, discharge compliance and environmental response. Consequences depend on storage, bypass, rainfall, receiving environment and recovery. Contract and regulatory mechanisms can differ from drinking water.

The transaction model should retain separate scenarios where service and liability pathways are different.

36. EMERGENCY OPERATION

Emergency cost can include temporary equipment, manual staffing, fuel, transport, specialist response, laboratory testing, security, communications and accelerated procurement. Some cost may be recoverable through insurance or public support, subject to terms and evidence.

The base model should avoid assuming recovery until eligibility, limits, deductibles and timing are reviewed.

37. RESTORATION CAPITAL

An incident can expose unsupported devices, weak segmentation or missing backups that require rapid replacement. Restoration capex can exceed the cost of repairing the immediate failure because the utility must rebuild to an acceptable architecture.

The diligence team should separate pre-existing remediation from incident-driven restoration. Transaction allocation may differ between the two.

38. REGULATORY CONSEQUENCE

Regulators can require assessment, remediation, evidence and incident reporting. In England and Wales, the Drinking Water Inspectorate reports that cyber resilience audits informed legal notices and PR24 cyber improvement plans, with Ofwat deliverables tied to those notices [8].

The financial case should examine current obligations, funded allowances, delivery milestones and potential enforcement. It should not assume the position of a named utility without evidence.

39. DISCLOSURE CONSEQUENCE

Public companies subject to SEC rules must disclose material cyber incidents and annual information on material cyber risk management, strategy and governance [9]. Other issuers and jurisdictions have different regimes.

Transaction teams should assess materiality governance, information controls and the interaction between regulatory, law-enforcement and market disclosure. Timely escalation matters even when the ultimate loss remains uncertain.

40. CONTRACTUAL CONSEQUENCE

PPP, concession, operating, wholesale, offtake and service contracts can impose availability, quality, notification, step-in, termination, indemnity and force-majeure terms. Cyber events may not receive automatic relief.

Legal diligence should map each scenario to contractual rights and payment consequences. Technology language that is disconnected from service standards can leave allocation unclear.

41. INSURANCE

Cyber, property, machinery, business interruption, liability and crime policies can respond differently. Coverage depends on insured event, exclusion, waiting period, sublimit, causation, security representation, notification and evidence.

Insurance should be modelled as a conditional recovery after deductible and delay. It does not replace controls, continuity or liquidity.

42. CASH-FLOW PATHWAYS

Cyber exposure can affect revenue, operating cost, working capital, capex, tax, insurance recovery, penalties, financing cost and distribution. Each pathway needs timing and accounting treatment. Service interruption may reduce collections slowly while emergency spending occurs immediately.

The model should avoid adding overlapping estimates for the same physical event.

43. PRICING MATRIX

The matrix below illustrates how technical evidence can be translated into transaction analysis. It does not estimate the probability or cost of a named incident.

Table 1. Cyber-physical exposure and transaction pricing pathways

Exposure	Evidence to test	Potential service effect	Financial pathway	Transaction response
Insecure remote access	Accounts, MFA, routes, logs and session tests	Unauthorised control or loss of visibility	Response, outage and restoration cost	Pre-close fix, covenant or escrow
Weak segmentation	Current diagrams, rules and path tests	Wider compromise across sites	Longer containment and recovery	Remediation capex and downside case
Unsupported controllers	Inventory, support status and spares	Configuration loss or extended outage	Replacement and downtime	Capex adjustment and reserve
Untested backups	Restore test and configuration coverage	Delayed return to service	Emergency cost and revenue effect	Completion gate and liquidity buffer
Limited manual fallback	Exercise and staffing evidence	Service deterioration during outage	Alternative supply and overtime	Operating covenant and contingency funding
Supplier concentration	Contracts, access and exit evidence	Loss of support or privileged compromise	Replacement, delay and transition	Consent, step-in and transition plan

44. BASE CASE

The base case should include funded recurring security, maintenance, licences, monitoring, exercises and lifecycle replacement required to operate the asset responsibly. Excluding normal cyber cost overstates sustainable cash flow.

The case should show whether current tariff, concession payment or budget covers the capability. A temporary remediation programme should not be mistaken for steady-state operating cost.

45. REMEDIATION CASE

Remediation capex should be tied to identified gaps, architecture, asset count, field work, integration, testing and outage windows. Vendor quotations and engineering estimates are stronger than generic cost per site.

The plan should sequence quick configuration changes, compensating controls and asset replacement. Dependencies can make the critical path longer than procurement alone.

46. INCIDENT DOWNSIDE

The downside case should model a coherent scenario, including service effect, detection, containment, manual operation, recovery, public response and cash timing. It should avoid claiming an unsupported frequency.

Break-even analysis can show the incident likelihood or duration at which an investment changes value. This keeps assumptions visible.

47. SEVERE PLAUSIBLE CASE

A severe plausible case tests survival, liquidity, essential service and financing protections. It may include simultaneous loss of OT visibility, corporate-system disruption and supplier unavailability. The objective is resilience, not a prediction.

The case should identify emergency authority, minimum cash, access to liquidity, insurance timing and conditions for lender or public intervention.

48. PROBABILITY DISCIPLINE

Historical incident frequencies can be sparse, differently defined and rapidly changing. A precise annual probability can create false confidence. Where credible local and sector evidence exists, it should retain its source and limitations.

Where probability is weak, scenario ranges, control evidence, break-even tests and decision thresholds can support capital allocation without fabricated precision.

49. DURATION DISCIPLINE

Loss duration depends on detection, isolation, manual capability, backups, equipment, specialists, communications and regulatory clearance. It should be decomposed into stages rather than entered as one arbitrary number.

Exercises and restoration tests can provide evidence for some stages. External approval or supply delays may remain scenario assumptions.

50. HYPOTHETICAL VALUATION BRIDGE

Consider an acquisition in which diligence identifies incomplete segmentation, unsupported controllers and untested recovery. The amounts below are hypothetical and use unspecified monetary units.

Table 2. Hypothetical cyber adjustment bridge for a water-utility transaction

Item	Base-case treatment	Downside treatment	Evidence gate	Possible deal response
Recurring security operations	Include in sustainable opex	Higher temporary staffing	Approved operating model	EBITDA normalisation
Segmentation programme	Identified capital plan	Delay and outage windows	Detailed design and bids	Price adjustment or funded plan
Legacy controller replacement	Lifecycle capex	Accelerated replacement	Inventory and vendor support	Escrow, capex covenant or seller work
Incident response	Contingency and exercise	Emergency cost and liquidity	Tested plan and call tree	Minimum liquidity covenant
Insurance recovery	Exclude until eligible	Apply deductible and delay	Policy and broker analysis	Coverage condition or reserve
Service-payment deduction	None in base case	Scenario-specific deduction	Contract interpretation	Indemnity or downside valuation

51. ENTERPRISE VALUE

Cyber exposure can affect maintainable cash flow, required capital, growth investment and risk. The valuation should adjust the affected inputs rather than apply a universal cyber discount. A specific remediation programme can be modelled as capex; recurring capability belongs in opex; scenario loss belongs in downside analysis.

Any residual risk premium should be explained and reconciled with explicit cash adjustments to prevent double counting.

52. DEBT CAPACITY

Lenders focus on service continuity, cash flow, insurance, liquidity, security and operator capability. A cyber incident can create immediate cash need before recovery. Debt sizing should test coverage and liquidity through the modelled restoration period.

The credit paper should identify critical controls, reporting, incident notification, capex commitments and conditions for draw or distribution.

53. PROJECT FINANCE

Project-financed utilities or PPPs depend on a bounded project company, long-term contract and defined risk allocation. Cyber obligations should align with performance standards, lifecycle budgets, insurance, relief, step-in and handback.

The model should test whether cyber remediation is an allowable cost, a project-company risk or a change in law. Ambiguity can transfer value unexpectedly.

54. ACQUISITION FINANCE

Acquisition lenders may rely on due diligence completed under time pressure. Material gaps should be converted into funded actions and post-close covenants with realistic dates. A broad representation that systems are secure provides limited credit protection.

Conditions precedent should focus on exposures that can create immediate loss or undermine recovery. Lower-priority improvements can enter the integration plan.

55. PPP ALLOCATION

Public authorities retain accountability for essential service even when private parties operate assets. The contract should define security standards, audit, incident coordination, data, access, change, liability, relief and termination.

Risk allocation should reflect control. The operator can manage configuration and response; government may control threat intelligence, emergency powers or sector coordination; equipment defects may sit with suppliers subject to contract.

Table 3. Illustrative allocation of cyber risk in a water PPP or concession

Risk	Party best placed to manage it	Evidence or contractual mechanism	Financing consequence
OT configuration and access	Operator	Baseline, change control, audit and incident duty	Operating covenant and remediation reserve
Legacy condition at transfer	Grantor and operator as agreed	Disclosed inventory, condition survey and funded plan	Price, grant or completion adjustment
Equipment security defect	Supplier subject to negotiated terms	Warranty, secure support, patch and replacement rights	Supplier concentration and contingency
New legal requirement	Allocated under change-in-law regime	Defined threshold and approval process	Tariff, payment or tenor adjustment
Essential-service continuity	Operator with public coordination	Tested fallback, emergency plan and step-in	Liquidity and distribution controls
State threat intelligence	Public authority and operator	Protected information-sharing protocol	Scenario update and directed action
Insurance placement	Project company	Minimum cover, broker review and renewal evidence	Deductible, sublimit and reserve treatment

56. PURCHASE AGREEMENT

The purchase agreement can address disclosed incidents, compliance, systems, controls, data, suppliers, insurance and remediation. Representations should be grounded in diligence and materiality. Specific indemnities or escrow may address identified legacy matters.

The buyer should preserve access to evidence and avoid drafting that interferes with secure incident response or lawful reporting.

57. WARRANTY AND INDEMNITY INSURANCE

Warranty and indemnity insurance can exclude known issues, forward-looking remediation and inadequate diligence. The policy should be reviewed against the actual cyber findings. Coverage assumptions should not replace negotiation of known exposures.

The transaction team should maintain a clean evidence trail showing questions, responses, exceptions and specialist review.

58. COMPLETION MECHANICS

Cyber events between signing and completion can affect material-adverse-change analysis, covenants, disclosure and closing conditions. The agreement should define notification and information rights without requiring disclosure that would increase operational risk.

Pre-close changes to remote access, network architecture or key suppliers should require controlled approval where material.

59. DAY-ONE CONTROLS

Day one should secure identity, privileged access, remote pathways, incident contacts, backups, network visibility and supplier authority. Integration should avoid connecting environments before pathways and consequences are understood.

The buyer needs the ability to operate safely while longer remediation proceeds. A hurried technology consolidation can increase exposure.

60. FIRST 100 DAYS

The first phase should confirm crown jewels, architecture and open incidents. The next should close critical access and exposure gaps, test backup and manual operation, and approve the remediation portfolio. The final phase should complete exercises, financing updates and board reporting.

Actions should have owners, cost, evidence and stop conditions. Completion should mean verified control operation rather than policy publication.

61. CAPITAL PRIORITISATION

Cyber capital competes with leakage, quality, resilience and growth investment. Prioritisation should combine service consequence, pathway evidence, control effectiveness, recovery and implementation feasibility. Statutory obligations can override a purely financial ranking.

The objective is the greatest reduction in material service and value exposure per constrained unit of capital, subject to minimum control requirements.

62. CONTROL ECONOMICS

The cost of a control includes technology, engineering, downtime, training, monitoring and lifecycle support. Benefit arises by reducing pathway, consequence, duration or recovery cost. A control can also enable digital operations or regulatory compliance.

The business case should avoid assigning the whole scenario loss to every control in the chain. Marginal and combined effects need distinction.

63. VALUE OF EVIDENCE

Additional evidence is valuable when it can change a material decision. A restore test may determine whether a liquidity reserve is sufficient. A path test may determine whether segmentation capex is needed. Evidence collection can itself create operational risk and should be authorised.

Testing should stop when further precision is unlikely to alter the transaction response.

64. DECISION MATRIX

Control evidence and consequence support four responses: accept within appetite, remediate before commitment, proceed with funded conditions, or redesign and defer. High consequence with weak evidence warrants stronger gating. Low consequence with reversible action may proceed under monitoring.

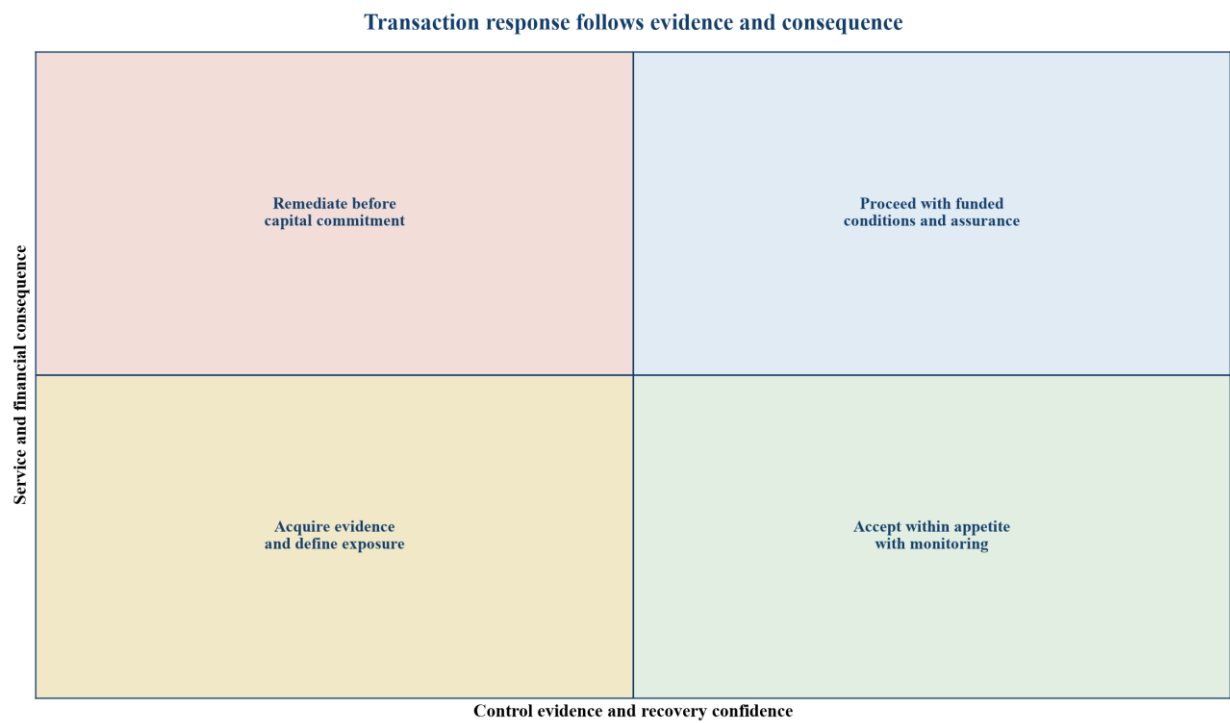


Figure 2. From OT control evidence to transaction response
Illustrative decision map; actual thresholds require utility, legal, regulatory and financing approval.

65. GOVERNANCE

The board owns oversight of material risk. Management owns the operating response. OT engineering, IT security, operations, asset management, finance, legal, risk, procurement and communications need defined roles. The SEC framework reinforces investor interest in management processes and board oversight for material cyber risk [9].

Technical teams should not carry commercial acceptance without authorised management judgement.

66. RISK APPETITE

Risk appetite should specify intolerable service and safety outcomes, minimum controls, maximum recovery conditions and escalation. A broad statement about low cyber risk is difficult to apply. The appetite should connect with enterprise risk, asset management and emergency planning.

Exceptions should state owner, duration, compensating controls and funded closure.

67. THREE LINES

Operations and technology teams own controls. Risk and compliance provide challenge and monitoring. Internal audit provides independent assurance. Specialist external review can supplement capability without transferring accountability.

The model should accommodate smaller utilities where people hold multiple roles by defining independent challenge for material decisions.

68. BOARD REPORTING

Reporting should show crown-jewel exposure, critical pathways, open incidents, control exceptions, recovery tests, overdue actions, supplier concentration, remediation spend and evidence of closure. Technical detail should remain available beneath concise decision information.

Trend data should use stable definitions. A falling vulnerability count can be misleading if asset discovery coverage also falls.

69. REGULATORY REPORTING

Incident and resilience reporting varies by jurisdiction. In England and Wales, qualifying operators report relevant NIS incidents without undue delay and within the stated regulatory timetable [2]. Other regimes have different triggers and authorities.

The response plan should maintain current legal advice and contact details. Deal teams should verify obligations rather than generalise from another market.

70. MANAGEMENT ASSUMPTIONS

Transaction models may require assumptions about incident duration, emergency cost, recovery, penalties and insurance. Each should be labelled, owned and tested. Unsupported sector averages should not be presented as target-specific facts.

The investment committee should see which assumptions reverse value, coverage or approval.

71. RED FLAGS

Red flags include unknown remote access, public-facing control devices, shared privileged accounts, unsupported controllers without isolation, missing logic backups, untested restoration, no manual fallback, outdated architecture diagrams, supplier access without contracts and cyber findings disconnected from the capital plan.

A material red flag should trigger evidence, remediation, transaction protection or a decision to defer.

72. DILIGENCE REQUEST LIST

The request list should cover architecture, inventory, access, vulnerability management, incidents, risk assessments, regulatory correspondence, insurance, suppliers, backups, recovery, exercises, capex, policies and board reporting. Sensitive information should be handled in a controlled room with need-to-know access.

The team should request evidence samples and demonstrations, not broad policy documents alone.

73. MANAGEMENT INTERVIEWS

Interviews should include operators, control engineers, IT security, asset management, finance, legal, procurement and executive owners. Questions should test actual events, exceptions and decisions. Consistent scripted answers can hide operational gaps.

The adviser should reconcile interview statements with logs, configurations, tickets, exercises and capital plans.

74. SITE VERIFICATION

Site visits can confirm architecture, physical access, device condition, local fallback, spares and operator practice. Safety and operational protocols apply. Testing should not disrupt the process.

Representative sampling should reflect criticality, age, geography and supplier diversity. One modern control centre may not represent remote stations.

75. REMEDIATION ROADMAP

The roadmap should separate immediate containment, foundational control, legacy replacement, recovery capability and continuous improvement. Each action needs owner, cost, dependency, outage window, evidence and approval gate.

Quick wins should not delay high-consequence engineering work. Legacy replacement should align with asset outages where safe and feasible.

Capital commitment follows evidence through six transaction gates

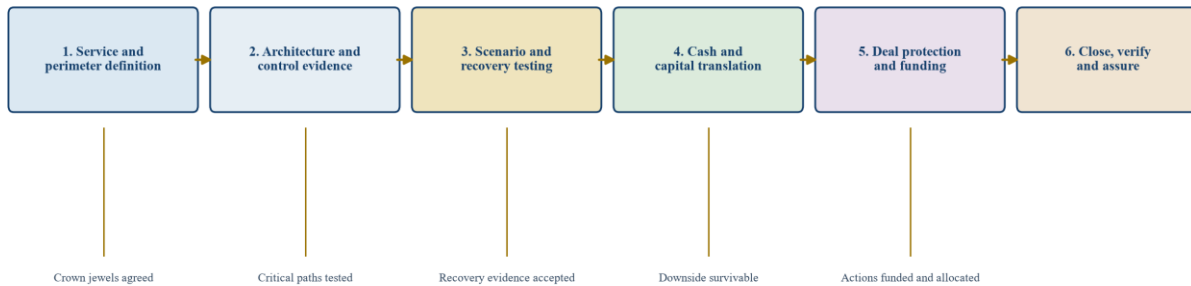


Figure 3. Stage-gated route from OT diligence to protected capital commitment

Generic transaction sequence; timing depends on evidence access, utility operations, regulation and deal structure.

76. FINANCING PROTECTIONS

Protections can include funded remediation, capex reserve, minimum liquidity, reporting, incident notification, insurance, independent assurance, distribution lock-up, completion test, supplier step-in and restrictions on material architecture change.

Each protection should address a defined exposure. Excessive generic covenants can create monitoring burden without improving resilience.

77. INVESTMENT-COMMITTEE PACK

The pack should include service perimeter, architecture, crown jewels, material scenarios, control evidence, recovery tests, regulatory obligations, contractual allocation, remediation capex, base and downside cash flows, insurance, financing protections, transaction terms and 100-day plan.

All management estimates should be identified. The committee should see unresolved evidence gaps and their decision consequence.

78. DECISION RULE

Proceed when essential services and critical pathways are understood, material controls are evidenced, safe fallback and recovery are credible, remediation is funded, cash downside is survivable and contracts allocate risk deliberately. Condition approval where closeable gaps have owners, money, timetable and verification.

Defer when unknown exposure or untested recovery could undermine service, value or financing and cannot be bounded before commitment.

79. CONTINUING ASSURANCE

Cyber exposure changes with threats, assets, suppliers and digital programmes. Controls require monitoring, exercises, architecture review and capital renewal. Acquisition diligence is a baseline for ownership, not a permanent conclusion.

Completed remediation should feed the asset register, valuation model, financing reports and board assurance.

80. CONCLUSION

Pricing OT exposure in a water utility requires a disciplined bridge from technical pathway to physical service, response, contract and cash. Generic scores and dramatic loss claims provide weak investment evidence. Architecture, control testing, recovery and accountable assumptions create a defensible basis for value.

The strongest transaction protects essential service first, funds known remediation, tests severe conditions and preserves liquidity and authority through recovery. Cyber diligence then becomes part of capital discipline rather than a separate technology checklist.

REFERENCES

- [1] National Institute of Standards and Technology. NIST SP 800-82 Rev. 3, Guide to Operational Technology Security. September 2023. <https://doi.org/10.6028/NIST.SP.800-82r3>
- [2] Drinking Water Inspectorate. The Network and Information Systems Regulations 2018. <https://www.dwi.gov.uk/the-network-and-information-systems-nis-regulations-2018/>
- [3] National Institute of Standards and Technology. NIST SP 1800-45, Cybersecurity for the Water and Wastewater Sector: Build Architecture. June 2026. <https://doi.org/10.6028/NIST.SP.1800-45>
- [4] Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency and Federal Bureau of Investigation. Top Cyber Actions for Securing Water Systems. February 2024. <https://www.cisa.gov/news-events/alerts/2024/02/21/cisa-epa-and-fbi-release-top-cyber-actions-securing-water-systems>
- [5] Cybersecurity and Infrastructure Security Agency. IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities. Revised December 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>
- [6] National Institute of Standards and Technology. NIST SP 1339, Operational Technology Backup Quick Start Guide. June 2026. <https://csrc.nist.gov/Projects/operational-technology-security/publications>
- [7] Cybersecurity and Infrastructure Security Agency, Environmental Protection Agency and Federal Bureau of Investigation. Incident Response Guide: Water and Wastewater Sector. January 2024. https://www.epa.gov/system/files/documents/2024-01/wws-sector_incident-response-guide.pdf
- [8] Drinking Water Inspectorate. Network and Information Systems: summary of the Chief Inspector's report for drinking water in Wales, 2025. <https://www.dwi.gov.uk/what-we-do/annual-report/drinking-water-2025/drinking-water-2025-summary-of-the-chief-inspectors-report-for-drinking-water-in-wales/network-and-information-systems-nis/>
- [9] United States Securities and Exchange Commission. Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Release No. 33-11216. July 2023. <https://www.sec.gov/rule-release/33-11216>
- [10] United States Environmental Protection Agency. Cybersecurity Assessments for Drinking Water and Wastewater Systems. <https://www.epa.gov/cyberwater/cybersecurity-assessments>
- [11] United States Environmental Protection Agency. Cybersecurity for the Water Sector. Updated September 2026. <https://www.epa.gov/cyberwater>
- [12] United Kingdom Government. Cyber Security and Resilience (Network and Information Systems) Bill: summary. Updated June 2026. <https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill>
- [13] Drinking Water Inspectorate. Enforcement Policy: Network and Information Systems. https://www.dwi.gov.uk/what-we-do/nis_enforcement_policy/

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 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.

LinkedIn: <https://www.linkedin.com/in/ckadya/>

Profile: <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.