Quantum Timing Infrastructure Finance Resilience as a Contracted Service

A Commercial and Capital Framework for Sovereign Telecom Financial Market and Critical Infrastructure Demand

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Precise time is a shared input to telecommunications, financial markets, power systems, data centres, transport and public safety. Much of the installed timing estate depends directly or indirectly on signals from global navigation satellite systems. Those signals are highly useful, widely available and vulnerable to interference, spoofing, space weather, system failure and common-mode dependence. Governments and standards bodies increasingly treat timing resilience as a critical-infrastructure requirement. The financing problem remains difficult because a national or network timing system combines public-good characteristics, specialist hardware, fibre and radio distribution, assurance operations, standards compliance and customer-specific integration. Scientific clock performance alone does not create a bankable service.

This paper develops a finance framework for resilient quantum and atomic timing infrastructure delivered as a contracted service. It begins with the customer continuity decision, maps the technical architecture from national time scale to the point of use, and separates laboratory accuracy from service availability, holdover, traceability, cyber security and operational acceptance. It considers sovereign and telecom anchor contracts, financial-market compliance, energy and transport use cases, data-centre distribution, wholesale service providers and public procurement. It also examines how contracts can allocate performance, demand, technology, integration and obsolescence risk.

The evidence base includes United Kingdom policy for greater positioning, navigation and timing resilience, the National Physical Laboratory National Timing Centre and NPLTime services, United States National Institute of Standards and Technology work on resilient timing and critical infrastructure, International Telecommunication Union standards for packet, frequency and phase synchronisation, European financial-market clock requirements, United States consolidated-audit-trail requirements, European Space Agency navigation programmes and public procurement notices. These sources establish real policy, standards and service-development activity. They do not establish uniform willingness to pay, a universal technical architecture or the bankability of any named project.

A wholly hypothetical operating case illustrates the commercial method. The model platform holds four sovereign or critical-infrastructure anchor contracts, eight telecom or network contracts, ten financial-market or data-centre connections and recurring assurance revenue. Central-case annual revenue is USD 24.40 million. Direct service, network, equipment and support cost is USD 13.70 million, leaving USD 10.70 million of contribution before central research, sales and corporate overhead. A pilot-heavy case produces USD 8.20 million of revenue and a contribution loss of USD 1.50 million. A scaled case produces USD 52.80 million of revenue and USD 24.20 million of contribution. These values are management assumptions used to demonstrate method; they are not observations about a named company or a market forecast.

The analysis concludes that resilient timing becomes financeable when contracts buy an observable continuity outcome. A credible service specifies the reference, distribution route, accuracy at the point of use, availability, holdover, monitoring, incident response, audit evidence and remedies. Public or regulated anchor demand can support shared infrastructure when commitment duration, payment security, change control and termination protection match the capital cycle. Growth capital should follow accepted service nodes, repeatable integration, contracted recurring revenue, proven operating cost and collected cash. Project or asset-backed capital becomes more plausible when hardware and network assets are separable, contracts are assignable and downside service obligations remain funded.

JEL Classification: G24, H54, L51, L63, L96, O31, O32, O33

Keywords: quantum timing, resilient PNT, atomic clocks, optical clocks, GNSS resilience, critical infrastructure, telecom synchronisation, contracted service, project finance, technology financing

Introduction

Digital infrastructure depends on a consistent order of events. Mobile networks coordinate radio resources. Power networks compare measurements across dispersed assets. Trading systems sequence orders and transactions. Data centres coordinate distributed workloads. Transport and public-safety systems use common time to align data, communications and control. A timing failure can therefore create more than a clock error. It can impair service continuity, forensic reconstruction, regulatory evidence and confidence in interconnected systems.

Global navigation satellite systems provide a convenient and highly capable timing source. Dependence becomes material when multiple systems use the same external signal and lack an independent reference or adequate holdover. NIST identifies energy, finance and transport among the critical sectors that need resilience to disruption of positioning, navigation and timing services [1]. The United Kingdom's current policy framework treats the loss of satellite-provided PNT as a national risk and promotes a system-of-systems approach that combines terrestrial and space-based sources [2,3].

Atomic and optical clocks can strengthen this architecture. Their role ranges from maintaining national time scales to providing holdover at network nodes or customer sites. The clock is one component. Distribution over fibre, packet networks, radio or satellite links; comparison between clocks; traceability to coordinated universal time; monitoring; cyber controls; and customer integration determine whether timing reaches the application with the required performance.

The commercial opportunity is therefore a service problem. Customers may pay for a traceable signal, a resilient second source, continuous monitoring, regulatory evidence, incident response or a complete managed timing system. The financing structure should reflect the service purchased, the shared infrastructure required and the residual risk retained by the provider. This paper develops a framework for that decision.

1 Define the continuity outcome before selecting the clock

The first financing question is which customer service must continue during degradation or loss of its primary timing source. A telecom operator may need phase and time synchronisation within a defined limit to maintain radio or transport-network performance. A trading venue may need traceability to UTC and evidence that its business clocks remain within the applicable divergence. A grid operator may need time-aligned measurements for disturbance analysis and protection. A data-centre operator may require trusted sequencing across distributed systems. These are different outcomes with different tolerances and liabilities.

The customer requirement should specify the point of measurement. Accuracy at the national laboratory, provider node or grandmaster does not prove accuracy inside the customer's application. Fibre delay, packet asymmetry, network reconfiguration, local oscillator behaviour, hardware timestamping,

environmental change and internal distribution can affect the delivered result [4-7]. The contract should therefore define where performance is measured, how it is verified and which components are included.

Continuity also requires a time horizon. A system may ride through seconds of packet loss, hours of local disruption or days of satellite unavailability. ITU describes enhanced primary reference clocks capable of maintaining high accuracy for extended periods after loss of their reference and a coherent network architecture that connects and compares clocks [6]. The useful holdover requirement depends on the customer's recovery plan and the probability of correlated failure.

The commercial team should record the operational consequence of failure. This may include network degradation, regulatory breach, inaccurate event reconstruction, curtailed services, unsafe operation or manual fallback. The value of resilience should be grounded in the avoided exposure and the customer's control obligation. Broad statements about national importance cannot substitute for a named decision owner, acceptance test and budget.

2 Map the service from reference time to point of use

A timing service begins with a reference. National metrology institutes maintain realisations of UTC and compare them internationally. The service then needs a dissemination path. NPL describes fibre, communication satellites, terrestrial broadcast and internet distribution within the United Kingdom timing programme [8]. NIST proposes resilient architectures that use the national time scale, diverse distribution and local systems rather than relying on one external source [9].

Distribution architecture determines both capital needs and risk. Dedicated fibre can provide high performance and clear control over the path, while requiring access, equipment, route diversity and maintenance. Packet-based timing can use telecom infrastructure but depends on network support, timestamping, asymmetry control and service configuration. Terrestrial radio can reach broad areas but involves spectrum, transmission assets, coverage and receiver integration. Satellite links can compare or distribute time over distance and remain exposed to their own interference and infrastructure risks.

At the customer site, equipment may include a receiver, grandmaster, boundary clocks, local oscillator, monitoring appliance, secure management system and interfaces to the application. A provider that stops at the access point may avoid part of the integration risk. A managed-service provider can earn more recurring revenue while accepting responsibility for the complete chain.

The architecture should show every dependency and control boundary. It should identify reference sources, comparison links, primary and alternate distribution routes, active and standby nodes, local holdover, monitoring, power, environmental control, cyber management and application interfaces. Financing should follow the cost and risk attached to those elements, not a generic quantum-technology category.

3 Separate clock capability from timing-service performance

Clock specifications can include frequency stability, phase noise, accuracy, drift, environmental sensitivity, size, power and holdover. Optical clocks and related frequency references can reach exceptional scientific performance. Commercial infrastructure also needs reliability, maintainability, standard outputs, calibration, remote management and supply continuity. ESA's NAVISP activity on optical precision time keeping explicitly connects an optical reference to synchronisation and dissemination through White Rabbit so it can function as a commercial stratum-one clock [10].

Service performance includes the complete system. Relevant measures can include time error at the delivery point, maximum time interval error, frequency offset, packet-delay variation, availability, switchover behaviour, holdover duration, alarm latency, restoration time and evidence retention. ITU

recommendations provide architectures, interfaces and performance concepts for telecom synchronisation [4-7]. They create a common basis for acceptance without prescribing one vendor solution.

The provider should maintain a claim register. Each performance statement should link to a configuration, environment, test method, comparator, uncertainty and acceptance record. Laboratory results should be separated from network demonstrations and live customer service. A test across one fibre route does not prove a national service. A clock that performs under controlled temperature does not prove field holdover. A successful pilot does not prove repeatable installation or support economics.

For valuation, capability should advance through evidence states: calibrated clock or frequency reference; integrated node; controlled distribution; representative network demonstration; accepted customer service; repeat contracted service; and scaled multi-sector operations. Each state should have a financing milestone and an explicit residual risk.

4 Design source diversity and holdover as an integrated control

Resilience requires independence that is meaningful for the relevant hazard. Two receivers using separate antennas can still share the same satellite constellation or local interference environment. Two packet routes can share fibre, power, software or network control. A terrestrial signal may rely on a common upstream reference. The architecture should identify common-mode dependencies across reference, distribution, power, cyber control and operations.

Source diversity can combine GNSS constellations, terrestrial timing, national-laboratory fibre, packet timing, satellite time transfer, eLORAN, local atomic clocks and monitored oscillators. The United Kingdom policy programme includes terrestrial sovereign timing and eLORAN as part of a broader system of systems [2,3,11]. The appropriate combination depends on required accuracy, geography, threat model and cost.

Holdover bridges a disruption. Its useful performance depends on oscillator quality, environmental control, calibration history and the duration of the outage. A provider should test holdover under the same environmental and operational conditions expected in service. The contract should define the start condition, accuracy envelope, alarm state and customer action when holdover approaches its limit.

Financing models should avoid paying indiscriminately for the highest available clock performance. A lower-cost device may satisfy a local requirement when supported by diverse references and rapid restoration. A more capable clock may be justified at an aggregation node serving many critical customers. The commercial design should place performance where it creates system value.

5 Translate standards into contract acceptance

Standards make timing performance legible to customers, regulators and investors. ITU defines telecom clock types, timing interfaces, packet profiles and network concepts that support frequency, phase and time distribution [4-7]. IEEE Precision Time Protocol and White Rabbit implementations provide additional mechanisms. Financial-market rules refer to UTC traceability, timestamping points and divergence limits [12-14]. These requirements should be translated into measurable contract terms.

The statement of work should identify the applicable standard and edition, service configuration, test equipment, sampling method, acceptance period and treatment of uncertainty. Compliance language should reflect the provider's actual scope. A signal provider may support a customer's compliance process without assuming responsibility for every clock inside the customer's estate. A managed-service provider may accept broader responsibility only when it controls the relevant equipment and network.

Service levels should distinguish availability from accuracy. A timing feed can remain reachable while outside its performance envelope. Conversely, a customer can maintain acceptable time during an upstream outage through local holdover. The service-level calculation should therefore use valid timing

rather than connectivity alone. Planned maintenance, customer-caused faults, force majeure and external-reference failures require precise treatment.

Remedies should match measurable loss and controllability. Service credits can address shortfalls in recurring service. Re-performance, replacement and corrective action can address equipment or integration failure. Broad consequential-loss exposure can overwhelm a young provider and undermine financeability. Liability caps, insurance, customer responsibilities and step-in rights should align with the criticality and contract value.

6 Build sovereign anchor demand around defined public outcomes

National timing infrastructure has public-good characteristics. A resilient reference and distribution network can support many sectors, while early demand may not recover the full capital cost. Government can act as funder, procuring authority, anchor customer, standards sponsor or owner of strategic assets. The chosen role affects competition, private investment and long-term operating incentives.

United Kingdom public material describes a nationally distributed timing infrastructure and a substantial public investment programme [8,15]. Procurement notices describe a resilient, terrestrial and sovereign timing signal and related operating capability [16]. These sources show a real policy and procurement pathway. They do not establish the final commercial structure or revenue available to any private supplier.

An anchor contract should define the public outcome, assets, coverage, performance, operational term and handback or renewal. Capital grants can fund non-recoverable research or strategic infrastructure. Milestone payments can support build and acceptance. Availability payments can support continuing operation. Usage charges can allocate variable cost or premium service. The mix should avoid double recovery and preserve incentives for uptime and adoption.

Termination and change protections matter because technology and policy can evolve faster than the asset life. The contract can compensate unrecovered approved capital following termination for convenience. Benchmarking and change control can address standards evolution. Open interfaces and asset registers can reduce lock-in while protecting legitimate intellectual property. Sovereign demand becomes financeable when public obligations, payment security and provider risk are clear.

7 Structure telecom anchor contracts around network deployment

Telecommunications can provide both demand and distribution. Mobile and fixed networks already manage synchronisation and operate sites, fibre, packet transport and monitoring. Timing standards provide a basis for specifications. A telecom operator can buy a wholesale reference, deploy provider equipment, integrate a managed service or offer assured timing onward to enterprise customers.

The contract should segment the network. Core nodes, aggregation sites, edge facilities and radio sites can require different performance and holdover. An initial deployment can prioritise nodes where one resilient reference supports many downstream services. Expansion can follow coverage, customer uptake and operational evidence.

Pricing may include installation, node capacity, managed-service subscription, monitoring, incident response and premium assurance. A minimum commitment can support shared capital. Volume bands can reduce unit price as connections scale. Take-or-pay terms may be appropriate where the provider reserves dedicated capacity or builds route-specific assets. The provider should avoid assuming unbounded site-integration cost under a fixed price.

NPL's collaboration with telecom operators and ITU's standards work provide evidence that terrestrial network distribution is an active development area [6,8]. Financing still depends on individual contracts. Investors should test contract duration, credit, renewal, change control, performance exclusions, equipment ownership, access rights and the operator's internal deployment plan.

8 Convert financial-market compliance into recurring service

Financial markets create a clear need for traceable and auditable time. European requirements address UTC traceability, the point at which timestamps are applied and maximum divergence [12]. United States consolidated-audit-trail requirements include business-clock synchronisation to NIST time, with tighter standards for certain market participants [13,14]. NPLTime provides terrestrial fibre timing to financial-sector users with service-level agreements [8].

The value proposition includes compliance evidence, operational resilience and event reconstruction. A provider can deliver a traceable source, monitored local distribution, independent comparison, audit reports and incident records. The customer may retain responsibility for timestamp placement and internal systems. The contract should clearly divide those controls.

Recurring revenue can be supported by multi-year connections, monitoring and assurance. Installation revenue should be separated from continuing service. Customer concentration can be significant if initial adoption comes from a small number of trading venues, data centres or service providers. Contracts should be assessed for assignment, renewal, price indexation and termination.

The provider should avoid treating regulatory need as automatic demand. Institutions may already satisfy requirements through existing systems. Switching requires integration, testing, governance approval and confidence in operational support. Commercial evidence therefore requires paid connections, completed acceptance, continued use and renewal rather than expressions of interest.

9 Develop energy transport and data-centre use cases separately

Energy systems use timing for synchrophasors, disturbance analysis, protection, event recording and distributed control. NIST's smart-grid work focuses on requirements, secure and resilient timing and monitoring under distributed conditions [17]. The criticality and accuracy requirement vary by application. A transmission control function should not be priced or contracted like a research data feed.

Transport use cases include network coordination, communications, signalling, autonomous systems and event reconstruction. Safety cases, certification and long asset lives can slow deployment. Public procurement or regulated operators may provide anchor demand. Interfaces with existing equipment and operational procedures can be more important than incremental clock performance.

Data centres and cloud infrastructure need consistent time for distributed systems, security logs, transactions and service management. Telecom timing can support physical infrastructure while software time protocols serve many applications. A resilient timing provider should state which layer it serves and the accuracy, trust and continuity delivered at that layer.

Each sector needs its own evidence plan, contract form and unit economics. Shared reference and distribution assets can create scale. Application integration, certification, support and liability remain sector specific. The provider should allocate common infrastructure cost transparently and avoid assuming that one anchor proves demand across all sectors.

10 Choose the commercial boundary and business model

The provider can sell equipment, access, managed service, assurance or a combined solution. Equipment sales create early cash but can fragment configurations and limit recurring revenue. Signal access can scale when distribution infrastructure exists and customer integration is simple. Managed service supports deeper recurring revenue and control but increases operating responsibility. Assurance services can include monitoring, calibration, reports, audit evidence and incident response.

A wholesale model can serve telecom operators, data centres or system integrators that resell timing. This reduces direct customer acquisition and can concentrate counterparty power. A direct model provides

application insight and pricing control while increasing support cost. A hybrid model can reserve national or network capacity for anchors and sell premium services to additional customers.

Asset ownership influences finance. Provider-owned clocks, nodes and network equipment can support recurring contracts and asset-backed structures when assets are identifiable and reusable. Customer-owned equipment reduces provider capital but may create integration variability. Publicly owned strategic assets can be operated under availability-based contracts.

The board should select a commercial boundary that matches its technical control, balance sheet and liability capacity. Revenue should be recognised according to actual performance obligations and acceptance terms. Development grants and reimbursed research should be separated from repeat service revenue [18].

11 Allocate construction integration and technology risk

Timing infrastructure can include specialised clocks, fibre access, network equipment, secure sites, environmental control, radio transmission, software and customer integration. Completion risk arises when these elements depend on different suppliers and acceptance tests. A financeable plan needs a baseline design, interface schedule, procurement plan and systems integrator.

Fixed-price engineering can transfer some cost risk when the scope is mature. Emerging technology and first-of-kind integration often require allowances, shared risk or staged design. The provider should avoid committing to national coverage or strict service levels before representative route and node tests are complete. Contingency should be linked to identified risks rather than an arbitrary percentage.

Technology risk includes performance, obsolescence, export controls, component availability and vendor concentration. Open interfaces can allow clock or distribution components to be upgraded. Configuration control and test automation reduce the cost of change. Source code, firmware, calibration methods and operational data require clear ownership and continuity rights.

Contracts should contain acceptance at component, node, route and service levels. Payment milestones should require objective evidence. The financing draw schedule should match procurement deposits, installation, testing and customer acceptance. Retention or performance security can protect the customer while preserving provider liquidity.

12 Build service operations and cyber assurance before scale

Timing is security-sensitive infrastructure. A false or manipulated time source can disrupt systems and obscure event sequences. Controls should cover device identity, secure management, configuration, software updates, access, logging, monitoring and incident response. Network and physical access should be controlled at reference, distribution and customer nodes.

Operational monitoring should compare sources, detect anomalies and identify drift before the customer breaches its limit. NIST's responsible-use work emphasises risk management for PNT services [1]. ITU's coherent network concept includes clock comparison and coordinated time-scale operation [6]. The provider should translate these principles into a monitored service.

Service operations require staffing, spare equipment, calibration, field support, escalation and customer communication. Availability commitments should be supported by route diversity, power resilience, maintenance procedures and recovery exercises. Insurance and business-continuity planning should reflect the service scope.

Investors should review evidence from live operations: alarms, incidents, time to acknowledge, time to restore, valid-service availability, holdover events, false alarms, maintenance, customer tickets and audit

findings. A technically strong system with immature operations should not be valued as established critical infrastructure.

13 Model unit economics by node connection and assurance tier

Unit economics should separate shared infrastructure from customer-specific cost. Shared cost can include national-reference access, core clocks, comparison links, network operations, security and product development. Node cost includes equipment, site access, installation, fibre or network capacity, power, environmental control and maintenance. Customer cost includes integration, acceptance, support, reporting and account management.

Revenue can be modelled by anchor contract, provider node, customer connection, assurance tier and professional service. The board should track contracted annual recurring revenue, installed recurring revenue, acceptance backlog, renewal, churn and collected cash. Usage measures may include active nodes, valid-service hours, monitored endpoints and premium incidents.

Contribution should include network charges, equipment depreciation or lease cost, field support, calibration, spares, hosting, licences and service operations. Gross margin can improve when one reference and distribution path serves additional customers. It can deteriorate when each customer requires a unique route, bespoke interface or high support burden.

Working capital can be material. Specialist hardware may require deposits and long lead times. Public and enterprise customers can pay after acceptance. The contract should align advance payments, milestones and recurring billing with procurement and deployment cash. A growth plan should show liquidity under delay and rework.

14 Use anchor contracts to finance shared infrastructure

An anchor contract can support capital when it provides minimum revenue, sufficient duration and acceptable payment credit. The contract should identify committed sites or capacity, deployment schedule, acceptance, indexation and termination compensation. Framework agreements without call-off commitments provide weaker support.

Shared infrastructure can be financed through corporate equity, vendor finance, equipment leases, project debt, government capital or blended structures. Corporate equity absorbs development and market risk. Vendor finance can match equipment payments to deployment. Leasing can fund identifiable standard assets. Project debt requires predictable cash flow, enforceable contracts and controlled completion risk. Public capital can fund strategic coverage or assets that private demand does not yet support.

Security may include project accounts, assignment of receivables, equipment charges, insurance proceeds and step-in rights. Critical service obligations can complicate enforcement. Lenders need continuity arrangements, cure periods and an operator-replacement plan. The public authority may restrict transfer or foreign control of strategic assets.

The financing structure should retain enough flexibility for technology upgrades. Overly rigid asset covenants can lock the service into obsolete equipment. A lifecycle reserve, permitted-upgrade regime and performance-based asset definition can protect both resilience and lender value.

15 Stage capital against evidence and contract gates

Early research capital should fund clocks, distribution methods, control software and controlled testing. Product capital should fund integrated nodes, representative routes, security and repeatable installation. Commercial capital should follow paid pilots, objective acceptance and signed anchor contracts. Infrastructure capital should follow design maturity, site rights, supply contracts and a credible operating model.

Milestones should be observable. Examples include traceable reference performance; defined holdover under representative conditions; successful source switchover; accepted point-of-use performance; completed cyber assessment; first paid service node; repeat installation; multi-year anchor commitment; and operating contribution.

The board should separate technical readiness from financeability. A clock can be technically mature while demand, contracts or delivery capability remain early. A public programme can provide strategic validation while leaving procurement timing uncertain. A customer pilot can prove integration while producing no repeat revenue.

Each financing round should fund the next evidence state with downside actions if milestones slip. The plan should state runway, committed spend, procurement cancellation rights, minimum operating capability and assets that retain value. This discipline reduces the risk that fixed infrastructure expands ahead of demand.

16 Apply scenario valuation to contracted evidence

Valuation should connect scenarios to evidence rather than apply a broad revenue multiple. A development scenario may contain intellectual property, team and funded research. A validated-service scenario adds integrated nodes and accepted performance. A contracted-platform scenario adds anchor commitments, installed recurring revenue and operating evidence. A scaled-infrastructure scenario adds diversified customers, renewals and predictable contribution.

Probability should reflect contract and execution evidence. A memorandum of understanding is weaker than an executed minimum commitment. A pilot acceptance is weaker than recurring service renewal. Public policy support is relevant and should not be counted as customer revenue until a contract exists. Grants and capital contributions should be separated from operating value.

The hypothetical scenarios in this paper produce a probability-weighted enterprise value of USD 204.25 million. The calculation is illustrative. It does not value a named company and does not represent a recommendation. Its purpose is to show how value can move as the evidence state changes.

Transaction diligence should reconcile contracts, revenue recognition, assets, service obligations, customer concentration, technology rights, standards compliance, cyber posture, supply chain, capital expenditure, working capital and downside liquidity. Any premium for strategic importance should be supported by competing demand, scarce capability or contractual control.

17 Prepare for procurement investment and transaction diligence

Public and critical-infrastructure procurement requires transparent scope, security, performance and governance. Bid materials should state the actual evidence base and avoid implying national coverage or regulatory compliance that has not been demonstrated. The provider should maintain a controlled response library linked to test reports, standards, certifications and contract positions.

Investor diligence should test whether revenue is commercial, grant-funded, reimbursed development or capital contribution. It should inspect acceptance clauses, termination, intellectual property, assignment, data rights, security obligations, insurance and liability. Pipeline should be separated by funded procurement, signed contract, paid pilot and uncommitted interest.

Technical diligence should reproduce key performance under representative conditions and examine the complete path to the point of use. Operational diligence should review monitoring, incidents, staffing, spares, calibration and recovery exercises. Financial diligence should rebuild node and customer economics from invoices, payroll, network contracts, asset registers and cash.

The service is investable when the evidence supports repeat delivery and a defensible commercial boundary. Strong science and policy relevance are important inputs. Contracted demand, accepted performance and controlled operations determine financeability.

18 Implement a ninety-day financing operating system

Days one to thirty should establish the service and evidence registers. Management maps references, nodes, routes, customer endpoints, configurations, standards, claims, test reports, incidents, contracts, invoices and cash. Every performance claim is linked to evidence and an accountable owner. Unsupported claims are removed or qualified.

Days thirty-one to sixty should build contract and unit-economics models. The team segments sovereign, telecom, finance, energy, transport and data-centre demand. It defines acceptance, service levels, installation cost, recurring direct cost, contribution, working capital and customer concentration. Opportunities are scored by funded need, technical fit, procurement path and contract quality.

Days sixty-one to ninety should complete scenarios and the financing plan. The board reviews design maturity, anchor commitments, deployment schedule, supply contracts, service operations, cyber assurance, downside liquidity and capital required to reach the next evidence state. Investment materials show assumptions, risks and disconfirming conditions.

The operating system continues after financing. Monthly reviews reconcile contracted and installed revenue, accepted nodes, valid-service availability, incidents, support, contribution and cash. Quarterly reviews update the architecture, standards register, contract risk, technology roadmap and scenario value.

Conclusion

Resilient timing is becoming a strategic infrastructure service. Government policy, national timing programmes, telecom standards and financial-market requirements provide credible demand signals. Commercial value still depends on converting those signals into contracted outcomes at the point of use.

A financeable service specifies reference, distribution, performance, holdover, monitoring, security, acceptance and remedies. It allocates integration and technology risk to parties that can manage them. Anchor contracts support shared infrastructure when duration, payment security, commitment and termination protection align with the capital cycle.

Investors, lenders, public authorities and acquirers should follow evidence states. Capital should move from research to integrated service, paid acceptance, anchor contracts, repeat deployment and scaled operations. The practical test is whether customers pay for a measurable continuity result and whether the provider can deliver that result repeatedly with controlled cost and risk.

Appendix A Minimum technical evidence schedule

Record the reference source, traceability chain, clock type, distribution route, interfaces, equipment configuration, software version, environment, power, cyber controls, measurement point, test method, instrument, uncertainty, result and acceptance. Test accuracy, stability, holdover, switchover, alarm, restoration and failure modes under representative conditions.

Maintain route and dependency maps. Identify shared fibre, power, sites, satellite links, software, suppliers and control systems. Record common-mode risks and compensating controls.

Appendix B Minimum contract evidence schedule

Record customer entity, service scope, sites, committed capacity, term, renewal, price, indexation, acceptance, service levels, exclusions, credits, liability, insurance, security, data rights, asset ownership, assignment, termination and change control. Separate binding commitments from options and forecasts.

Track procurement stage, funding approval, signature, deployment, acceptance, recurring billing, collection, renewal and expansion. Link each opportunity to technical fit and delivery capacity.

Appendix C Financial controls

Reconcile contracted annual recurring revenue, installed recurring revenue, installation revenue, grants, development contracts, capital contributions and cash. Allocate reference, network, equipment, site, field support, calibration, cyber, hosting, spares and operations cost by service line.

Track deposits, inventory, work in progress, deferred revenue, receivables, capital expenditure, lease obligations and lifecycle reserves. Stress acceptance delay, customer concentration, network cost, component lead time, service failure and renewal.

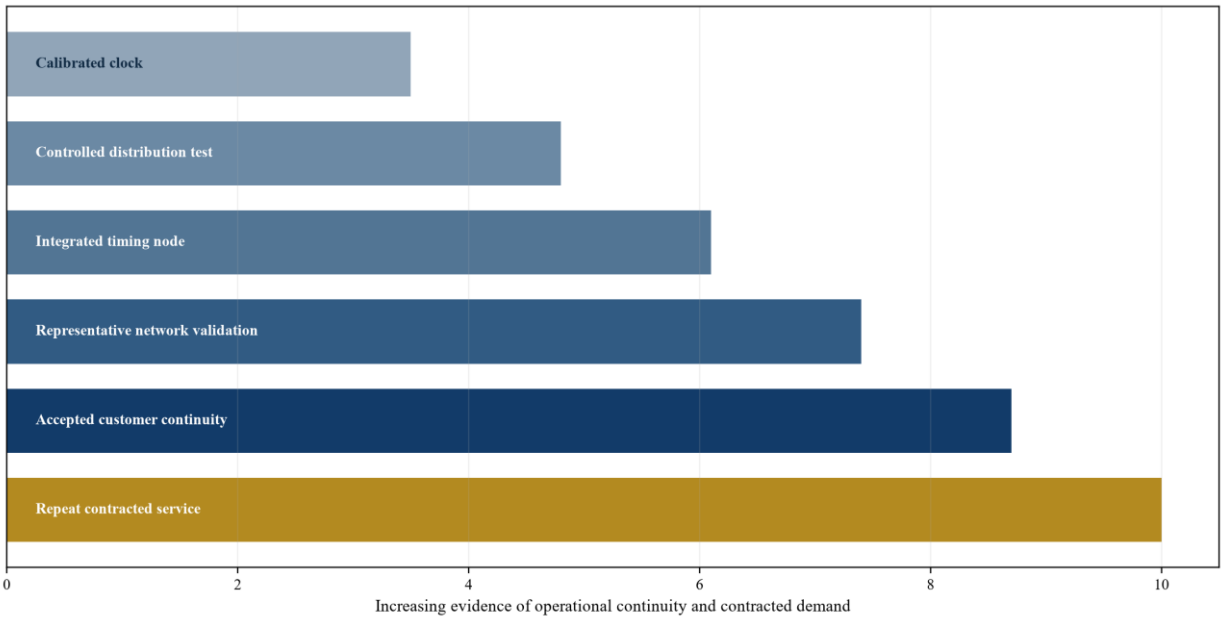
Appendix D Commercial evidence ledger

For each service record the customer continuity decision, timing tolerance, duration, architecture, point of measurement, comparator, evidence state, acceptance, contract, economics, rights and next gate. Link the ledger to the claim register, asset register, pipeline, incident record and financing milestones.

The board should distinguish observed performance, contracted commitments and hypothetical assumptions. Values without controlled evidence should be removed.

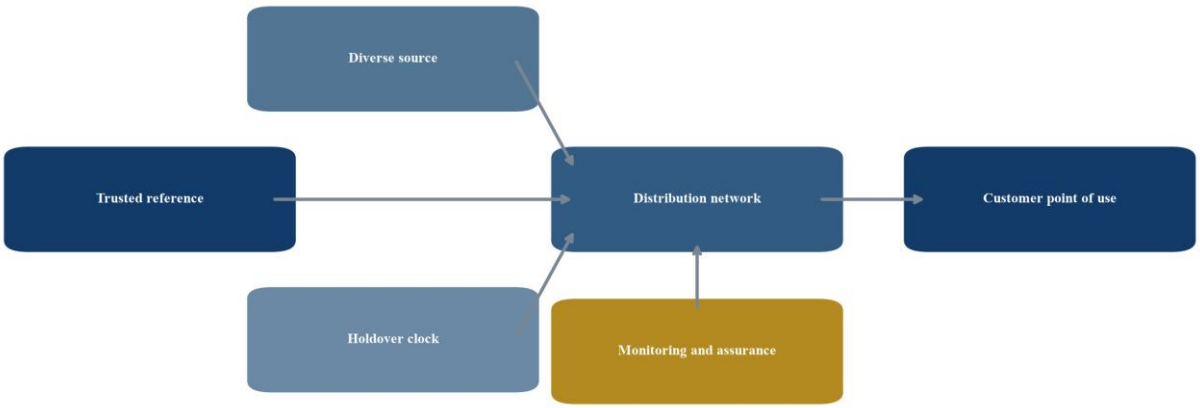
Appendix E Decision figures and tables

Figure 1. Resilient timing commercial evidence ladder



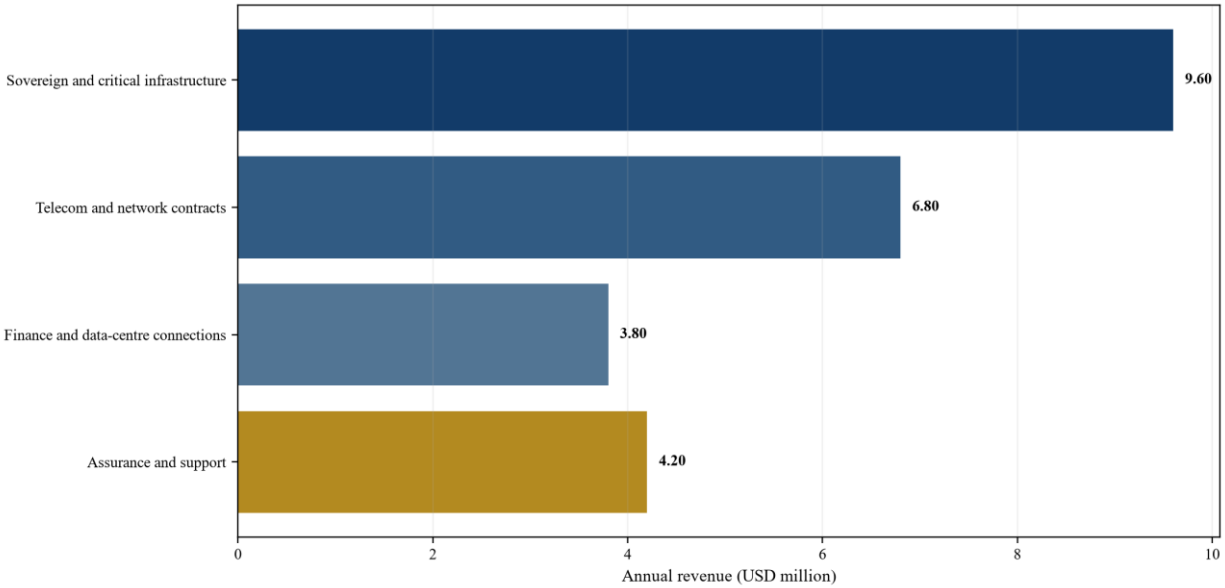
Proposed progression from calibrated clock to repeat contracted continuity service.

Figure 2. Proposed contracted timing service architecture



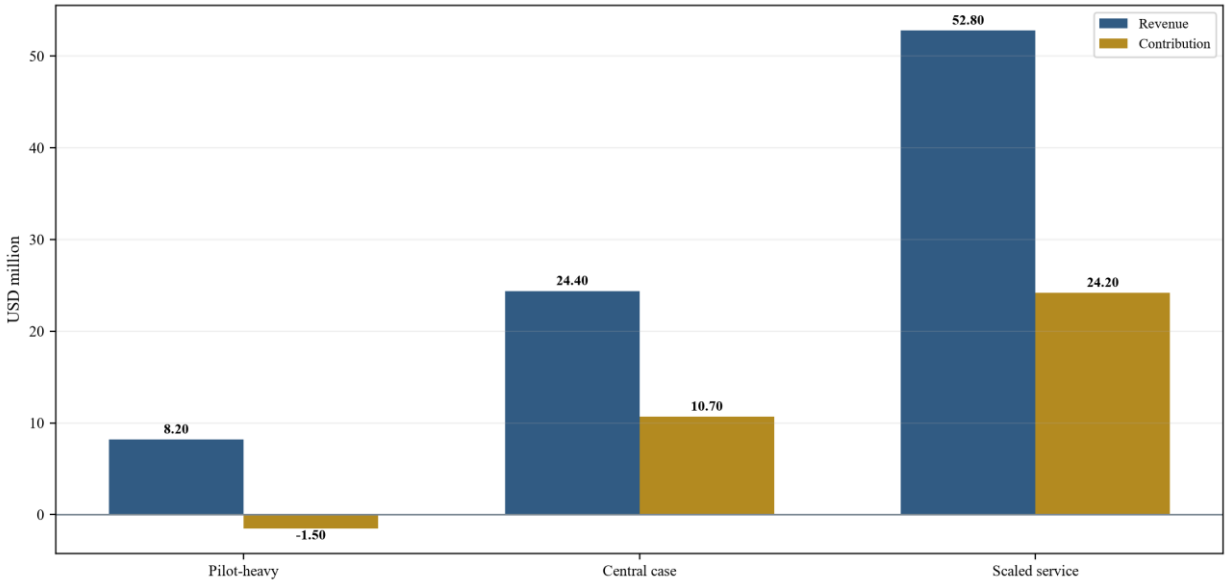
Performance is measured from trusted reference through distribution to the customer's point of use.

Figure 3. Hypothetical central-case revenue mix



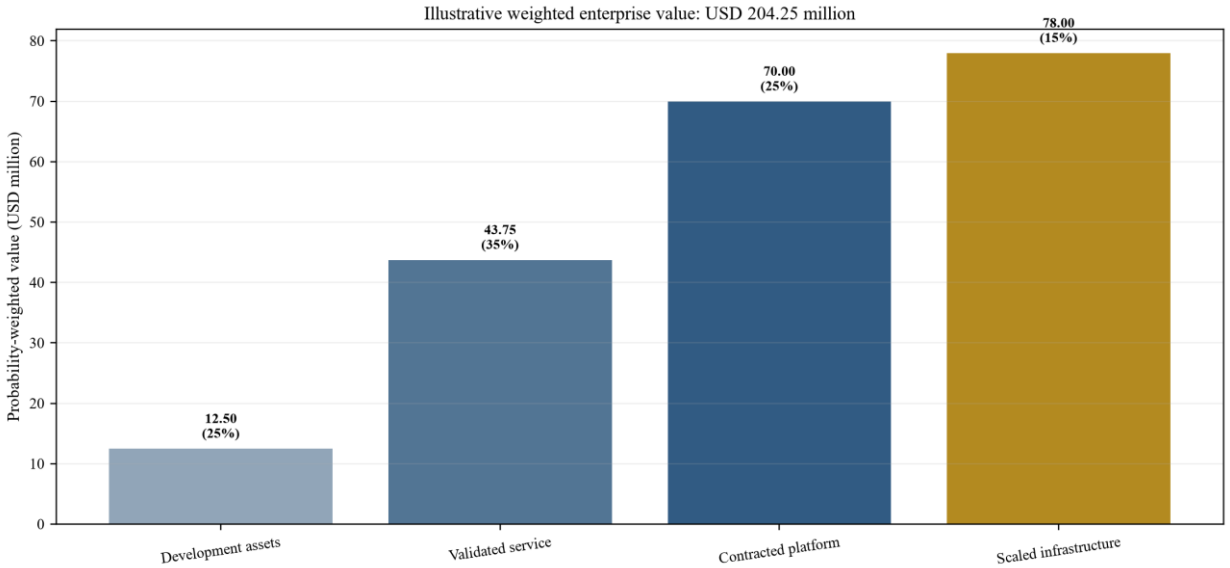
Wholly hypothetical management assumptions; USD million.

Figure 4. Hypothetical annual revenue and contribution by scenario



Wholly hypothetical management assumptions; USD million.

Figure 5. Hypothetical probability-weighted enterprise value



Wholly hypothetical management assumptions; USD million.

Table 1. Contracted timing evidence ladder

Level	Required evidence	Principal residual risk	Capital treatment
Calibrated clock	Traceable frequency and time measurement	System performance unproved	Research capital
Controlled distribution test	Known route, interfaces and repeatability	Representative network conditions	Product-development capital
Integrated timing node	Reference, holdover, monitoring and secure management	Operational reliability	Integration capital
Representative network validation	Point-of-use performance and failure testing	Scale and customer integration	Validation capital

Level	Required evidence	Principal residual risk	Capital treatment
Accepted customer continuity	Paid service and documented acceptance	Renewal and contribution	Commercial capital
Repeat contracted service	Multiple customers, routes and operating periods	Concentration and scaling	Growth or infrastructure capital

Proposed financing and valuation classification.

Table 2. Customer requirement scorecard

Dimension	Required evidence	Common weakness	Decision question
Continuity outcome	Named service and accountable owner	General resilience statement	What must continue?
Point of use	Defined measurement location and interface	Reference accuracy treated as delivered performance	Where is time verified?
Duration	Outage and holdover requirement	No recovery horizon	How long must the service bridge disruption?
Independence	Source, route, power and control diversity	Two sources with common dependencies	Which failure is mitigated?
Contract	Funding, commitment, acceptance and remedies	Pilot interest without budget	Who pays and for what?
Economics	Installed cost, recurring direct cost and value	Strategic importance without unit economics	Does the service create contribution?

Proposed qualification for resilient timing opportunities.

Table 3. Sector timing-service benchmark

Sector	Principal timing need	Evidence emphasis	Commercial route
Telecommunications	Frequency, phase and time across network	ITU profile, holdover, node acceptance	Wholesale or managed network service
Financial markets	UTC traceability and auditable timestamps	Point of timestamp, divergence and records	Fibre connection and assurance subscription
Energy	Distributed measurement and event alignment	Secure monitoring, field conditions and recovery	Utility contract or regulated programme
Data centres	Trusted time for distributed infrastructure	Service availability, cyber controls and integration	Facility or cloud service contract
Public infrastructure	Sovereign continuity and broad coverage	System-of-systems resilience and operations	Procurement, concession or availability payment

General comparison; actual requirements depend on application and jurisdiction.

Table 4. Hypothetical central-case revenue and contribution

Revenue or cost item	Units or basis	Revenue	Direct cost
Sovereign and critical-infrastructure anchors	4 contracts at 2.40	9.60	5.40
Telecom and network contracts	8 contracts at 0.85	6.80	3.80
Finance and data-centre connections	10 connections at 0.38	3.80	2.10
Assurance and support	Monitoring, reports and incident support	4.20	2.40

Revenue or cost item	Units or basis	Revenue	Direct cost
Total	Central case	24.40	13.70
Contribution before central overhead	Revenue less direct cost	10.70	

Wholly hypothetical management assumptions; USD million.

Table 5. Hypothetical operating scenarios

Scenario	Revenue	Contribution before central overhead	Principal condition
Pilot-heavy	8.20	-1.50	Demonstrations remain bespoke and anchor commitments are delayed
Central case	24.40	10.70	Four anchors, repeatable network deployment and recurring assurance
Scaled service	52.80	24.20	Diversified anchors, wholesale channels and productive shared infrastructure

Wholly hypothetical management assumptions; USD million.

Table 6. Hypothetical enterprise-value scenarios

Scenario	Evidence state	Enterprise value	Probability	Weighted value
Development assets	Transferable science, intellectual property and team	50	25%	12.50
Validated service	Integrated nodes and representative network acceptance	125	35%	43.75
Contracted platform	Anchor commitments, installed service and contribution	280	25%	70.00
Scaled infrastructure	Diversified renewals and predictable operations	520	15%	78.00
Total	Probability-weighted enterprise value		100%	204.25

Wholly hypothetical management assumptions; USD million.

Table 7. Board financing and transaction checklist

Decision question	Minimum evidence	Owner	Gate
Is the continuity outcome defined?	Service, tolerance, duration and accountable owner	Commercial and technical leads	Opportunity qualification
Does the end-to-end architecture perform?	Point-of-use test, holdover, monitoring and representative route	Technical committee	Product claim
Is anchor demand binding?	Funding, executed commitment, acceptance and payment security	Commercial and legal leads	Infrastructure commitment

Decision question	Minimum evidence	Owner	Gate
Can the service be operated securely?	Cyber controls, staffing, spares, incidents and recovery exercises	Operations leadership	Service activation
Does deployment create contribution?	Accepted nodes, recurring revenue, direct cost and collected cash	Finance and commercial leads	Growth funding
Can downside liquidity be funded?	Runway, working capital, reserves and staged actions	Board and finance	Capital release

Proposed governance control.

Frequently asked questions

What makes resilient timing a financeable service?

Financeability requires a defined continuity outcome, objective point-of-use performance, contracted demand, a credible operating model and cash flows that match the capital cycle. Strategic importance alone does not establish repayment capacity.

Are atomic or optical clocks sufficient on their own?

No single clock establishes a resilient service. Reference traceability, diverse distribution, holdover, monitoring, security, operations and customer integration determine whether usable time reaches the application.

Which customers can act as anchors?

Sovereign authorities, telecom operators, financial-market infrastructure, utilities and major data-centre providers can act as anchors when they make funded minimum commitments with adequate duration and credit.

How should a service-level agreement measure performance?

It should measure valid timing at the defined delivery point, including accuracy or time error, availability, holdover, alarm, restoration, evidence and exclusions. Connectivity alone is insufficient.

When can project or asset-backed debt be considered?

Debt becomes more plausible after design maturity, accepted deployment, enforceable anchor contracts, identifiable assets, predictable contribution, assignment rights and funded continuity obligations.

How should public funding be treated?

Research grants, capital contributions, milestone payments and operating revenue should be recorded separately. Public support can reduce development or strategic-infrastructure risk, while repayment capacity still depends on contracted cash flow.

What operating metrics matter most?

Track accepted nodes, valid-service availability, point-of-use performance, holdover events, incidents, restoration, contracted and installed recurring revenue, direct cost, contribution, concentration, renewal and cash collection.

What should the board review every quarter?

The board should review architecture dependencies, standards, claims, test evidence, anchor contracts, deployment, incidents, cyber controls, service economics, working capital, customer concentration and milestones for the next capital release.

References

[1] National Institute of Standards and Technology. Responsible Use of Positioning Navigation and Timing Services. 2026. https://www.nist.gov/pnt

[2] Department for Science Innovation and Technology. Positioning Navigation and Timing Overview. Updated 2 February 2026. https://www.gov.uk/guidance/positioning-navigation-and-timing-overview

[3] United Kingdom Space Agency. Corporate Plan 2025 to 2026 Theme 8 Positioning Navigation and Timing. 2025. https://www.gov.uk/government/publications/uk-space-agency-corporate-plan-2025-26

[4] International Telecommunication Union. ITU-T G.8271 Amendment 1 Time and Phase Synchronization Aspects of Telecommunication Networks. 2024. https://www.itu.int/epublications/publication/itu-t-g-8271-y-1366-2020-amd-1-2024-08

[5] International Telecommunication Union. ITU-T G.8273.4 Timing Characteristics of Telecom Boundary Clocks and Telecom Time Synchronous Clocks. 2024. https://www.itu.int/epublications/publication/itu-t-g-8273-4-2024-08-timing-characteristics-of-telecom-boundary-clocks-and-telecom-time-synchronous-clocks-for-use-with-partial-timing-support-from-the-network

[6] International Telecommunication Union. New ITU Clock Concept for More Resilient Synchronization Networks. 13 March 2024. https://www.itu.int/hub/2024/03/new-itu-clock-concept-for-more-resilient-synchronization-networks/

[7] International Telecommunication Union. ITU-T G.8275.2 Amendment 2 Precision Time Protocol Telecom Profile for Phase and Time Synchronization. 2024. https://www.itu.int/epublications/publication/itu-t-g-8275-2-y-1369-2-2022-amd-2-2024-08

[8] National Physical Laboratory. National Timing Centre Programme. Updated 2026. https://www.npl.co.uk/ntc

[9] National Institute of Standards and Technology. A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States. 2021. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933488

[10] European Space Agency NAVISP. Optical Precision Time Keeping. 2025. https://navisp.esa.int/project/details/346/show

[11] Department for Science Innovation and Technology. Critical Services to Be Better Protected from Satellite Data Disruptions through New PNT Framework. 18 October 2023. https://www.gov.uk/government/news/critical-services-to-be-better-protected-from-satellite-data-disruptions-through-new-position-navigation-and-timing-framework

[12] European Commission. Commission Delegated Regulation EU 2025 1155. 2025. https://eur-lex.europa.eu/eli/reg_del/2025/1155/oj

[13] United States Securities and Exchange Commission. SEC Seeks Public Comment on Plan to Create a Consolidated Audit Trail. 27 April 2016. https://www.sec.gov/newsroom/press-releases/2016-77

[14] United States Securities and Exchange Commission. Statement on Order Approving the Consolidated Audit Trail National Market System Plan. 15 November 2016. https://www.sec.gov/newsroom/speeches-statements/white-statement-open-meeting-111516html

[15] Department for Science Innovation and Technology and National Physical Laboratory. Cutting Edge Timing Technology to Protect Vital Services. 7 March 2026. https://www.gov.uk/government/news/cutting-edge-timing-technology-to-protect-vital-services

[16] Department for Science Innovation and Technology. National Timing Centre Delivery Programme Pipeline Notice. 22 May 2025. https://www.find-tender.service.gov.uk/Notice/024464-2025

[17] National Institute of Standards and Technology. Precision Timing for Smart Grid Systems. 2026. https://www.nist.gov/programs-projects/precision-timing-smart-grid-systems

[18] International Financial Reporting Standards Foundation. IFRS 15 Revenue from Contracts with Customers. 2026. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[19] International Telecommunication Union. ITU-T G.8265.1 Precision Time Protocol Telecom Profile for Frequency Synchronization. 2022. https://www.itu.int/rec/T-REC-G.8265.1-202211-I/en

[20] European Space Agency. ESA Navigation at 2025 Ministerial Council. 2025. https://www.esa.int/Applications/Satellite_navigation/ESA_Navigation_at_2025_Ministerial_Council

[21] National Institute of Standards and Technology. Timing Infrastructure. 2026. https://www.nist.gov/itl/ai/timing-infrastructure

[22] United Kingdom Space Agency. Annual Report and Accounts 2025 to 2026. 2026. https://www.gov.uk/government/publications/uk-space-agency-annual-report-and-accounts-2025-2026

[23] Department for Science Innovation and Technology. Robust Global Navigation System Project for Defence. 2026. https://www.gov.uk/guidance/robust-global-navigation-system-project-to-deliver-a-precise-source-of-position-velocity-and-time-information-for-defence

[24] National Physical Laboratory. NPLTime Financial Services. 2026. https://www.npl.co.uk/products-services/time-frequency/npltime

[25] National Physical Laboratory. Time and Frequency Services. 2026. https://www.npl.co.uk/products-services/time-frequency

[26] European Space Agency NAVISP. Work Plan 2025. 2025. https://navisp.esa.int/uploads/files/documents/NAVISP%20Element%201%20Workplan%202025%20web%20release.pdf

[27] Department for Science Innovation and Technology. United Kingdom eLORAN Market Engagement. 2025. https://www.find-tender.service.gov.uk/Notice/027816-2025

[28] International Organization for Standardization. ISO 27001 Information Security Management Systems. 2022. https://www.iso.org/standard/27001

[29] World Intellectual Property Organization. PATENTSCOPE Patent Search. 2026. https://www.wipo.int/patentscope/en/

[30] United States Department of Commerce Bureau of Industry and Security. Export Administration Regulations. 2026. https://www.bis.gov/regulations/ear

[31] International Financial Reporting Standards Foundation. IAS 16 Property Plant and Equipment. 2026. https://www.ifrs.org/issued-standards/list-of-standards/ias-16-property-plant-and-equipment/

[32] International Financial Reporting Standards Foundation. IFRS 16 Leases. 2026. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-16-leases/

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.

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.