Post-Quantum Migration for Satellite Fleets: Capex, Timing and Residual-Value Risk

A Fleet-Level Investment Framework for Cryptographic Discovery, Migration and Asset Value

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Satellite operators face a capital-allocation problem that is easy to misstate. The relevant question is not when a cryptographically relevant quantum computer will arrive. The decision is when each fleet element must become capable of replacing quantum-vulnerable public-key cryptography without compromising mission safety, interoperability, customer commitments or cash generation. Long design cycles, infrequent hardware replacement, constrained on-board computing, controlled software updates and customer accreditation make space assets different from ordinary enterprise systems.

This paper develops a fleet-level framework for post-quantum migration. It separates cryptographic discovery, ground-system remediation, software-signing changes, command-authentication changes, payload and customer-interface changes, on-board hardware constraints, certification, operational rehearsal and contingency. The framework treats migration as a sequence of evidence gates. It connects each gate to capex, operating cost, service availability, contract renewal, insurance, financing covenants and residual value.

The framework draws on NIST's final FIPS 203, FIPS 204 and FIPS 205 standards; NIST transition and crypto-agility work; NSA, CISA, United Kingdom and European migration guidance; NASA space-system protection requirements; CCSDS space-data-link security standards; and current ESA and ENISA work on satellite security. These sources support immediate discovery and staged migration. They do not establish the quantum-readiness, remaining life or value of any identified satellite fleet.

A wholly hypothetical fleet demonstrates the method. The operator has 42 spacecraft, 11 ground sites and 6 customer gateways. Eighteen newer spacecraft can support software changes with moderate engineering. Fourteen require gateway compensation and constrained hybrid operation. Ten older spacecraft cannot accept the preferred post-quantum algorithms without hardware or mission risk. The illustrative programme requires USD 146 million of nominal expenditure over seven years. Evidence-weighted planning classifies USD 82 million as committed or high-confidence capex, USD 39 million as conditional engineering and customer-accreditation spend, and USD 25 million as contingency. A delay of three years preserves near-term cash but reduces the hypothetical fleet's residual value by USD 238 million through shorter contractability, concentrated replacement needs and weaker terminal assumptions.

The central conclusion is that post-quantum migration should be underwritten as a fleet-modernisation programme. Value follows verified cryptographic inventory, upgrade paths, reversible testing, customer acceptance, protected command authority and funded retirement decisions. A board can preserve residual value by separating assets that can migrate, assets that need compensating controls and assets that should be harvested or retired; then aligning capex with mission life and contract value.

JEL Classification: G31, G32, L63, L96, O32, O33, Q55

Keywords: post-quantum cryptography, satellite fleet, cryptographic agility, capex, residual value, ground segment, command authentication, secure boot, mission assurance, space finance

Introduction

Public-key cryptography supports identity, key establishment, digital signatures, secure boot, software updates, command authentication, customer interfaces and administrative access across modern satellite systems. A future quantum computer capable of breaking widely used public-key schemes would affect several of those functions. The economic exposure begins earlier because long-lived data can be collected now, procurement and accreditation take years, and a spacecraft launched with a rigid cryptographic design may remain in service after current algorithms are deprecated.

NIST finalised ML-KEM, ML-DSA and SLH-DSA in 2024. Its migration programme focuses on cryptographic visibility, risk management, interoperability and benchmarking. The United Kingdom's National Cyber Security Centre recommends completing discovery and initial planning by 2028, high-priority migration by 2031 and broad completion by 2035. The European roadmap calls for Member States to start transition by the end of 2026 and protect high-risk use cases by the end of 2030. These dates provide planning anchors. Fleet decisions still depend on asset life, mission criticality, implementation readiness and the ability to change a live system safely.

This paper converts that policy direction into a capital and valuation framework. It distinguishes unavoidable security work from optional enhancement, identifies where capex can extend contractable life, and shows how migration delays can damage terminal value even when no quantum incident occurs.

1 Define the board decision

The board decision should specify the protected outcomes. Typical outcomes include maintaining authorised command, protecting customer and mission data, validating software and firmware, preserving regulatory eligibility, sustaining insurance and financing, and retaining the ability to renew contracts. The programme should not begin as an undifferentiated technology budget.

The decision perimeter covers spacecraft, payloads, ground stations, mission-control systems, customer gateways, identity systems, software-development and signing infrastructure, key-management systems, supplier interfaces and recovery facilities. Shared services belong in the perimeter when a failure or migration error can affect mission operations.

The board should approve three classifications. Assets in the migrate class have a technically and commercially justified upgrade path. Assets in the compensate class rely on protected gateways, shorter credential life, operational procedures or other bounded controls. Assets in the harvest-or-retire class cannot support an acceptable end state at reasonable cost. Each classification needs evidence, cost, timing, accountable ownership and an explicit residual-value treatment.

2 Start with cryptographic discovery

Cryptographic discovery is the first investable deliverable. The inventory should identify algorithms, protocols, keys, certificates, libraries, hardware modules, trust anchors, signing systems, interfaces and data lifetimes. It should show where cryptography is implemented, who controls it, which software version uses it and which customer or authority must approve a change.

Automated discovery can cover conventional infrastructure and software repositories. Spacecraft and specialised ground systems often require engineering review because cryptography may be embedded in firmware, field-programmable logic, radio equipment, command databases or proprietary interfaces. Procurement records and supplier attestations help identify components whose internal behaviour is not visible to the operator.

The inventory should be configuration controlled. A list assembled for a board paper becomes obsolete when software releases, certificates, customer gateways or supplier components change. The useful asset is a maintained relationship between configuration, cryptographic dependency, mission service, data sensitivity, replacement path and evidence owner.

3 Map cryptography to mission consequences

Not every cryptographic dependency has the same economic consequence. A public website certificate can be replaced through normal operations. A spacecraft root of trust may be fixed in hardware. A software-signing key can determine whether an emergency patch is accepted. A command-authentication mechanism can determine whether the operator retains positive control.

Each dependency should be mapped to confidentiality, integrity, authentication, non-repudiation, key establishment or software assurance. The map should then identify the affected mission function, outage tolerance, compromise consequence, data lifetime and recovery route. NASA requires protection of command authority across the end-to-end command path and recognises the spacecraft, ground segment and supporting services as one system of systems.

This mapping creates the economic priority. A dependency receives early funding when failure would interrupt material revenue, breach a customer requirement, prevent safe software updates or destroy recovery options. Low-consequence dependencies can be upgraded through routine refresh.

4 Separate the fleet into migration archetypes

Fleet age alone is an incomplete guide. Two spacecraft launched in the same year can have different processors, memory, radios, secure boot, update paths and mission constraints. The operator should classify assets by observed technical characteristics.

The first archetype supports software-defined cryptography, sufficient memory and processing, safe rollback and a tested update path. The second supports selected changes but requires careful optimisation, hybrid schemes or gateway assistance. The third has limited change capacity and depends on external compensation. The fourth lacks a credible protected path and should be evaluated for early replacement or constrained operation.

The classification should be configuration specific. Engineering should record the hardware revision, flight software, cryptographic library, boot chain, communications protocol, key-management interface and available resources. A management statement that a satellite is software defined does not establish that its trust anchor or command-authentication mechanism can be changed.

5 Distinguish ground, link and on-board migration

Ground infrastructure usually offers the fastest path to improved visibility and cryptographic agility. Identity, public-key infrastructure, key management, software signing, secure development, administrative access and customer gateways can often be upgraded before the spacecraft. This work creates inventory and operational experience while reducing exposure in the most accessible part of the system.

The space link requires protocol and interoperability decisions. CCSDS security standards provide structured authentication and confidentiality at the data-link layer. Post-quantum algorithms introduce different key, signature and message sizes, computation and implementation requirements. Operators must test the full path, including framing, bandwidth, error handling, latency, ground equipment and spacecraft software.

On-board migration is the most constrained. The design may rely on fixed hardware, stateful memory, narrow communication windows or safety-certified software. A technically possible algorithm

replacement can still be commercially impractical when it consumes scarce power, payload time or operating margin.

6 Build the target cryptographic architecture

The target architecture should identify the algorithms and protocols intended for each use case, including key establishment, digital signatures, secure boot, update signing, command authentication, telemetry protection, operator identity and customer interfaces. NIST's FIPS 203, 204 and 205 provide standardised building blocks. Protocol profiles and validated implementations remain necessary for deployed systems.

The architecture should preserve algorithm replacement. Crypto-agility requires more than a configurable name. It requires bounded interfaces, version negotiation, key and certificate lifecycle, policy, telemetry, rollback, test vectors and an authority that can retire an algorithm. The operator should avoid embedding new dependencies that will be as difficult to change as the old ones.

Hybrid operation may be appropriate during transition. The design should state what security claim the hybrid mechanism supports, how failure of either component is handled, and when the classical component can be removed. Compatibility should not become permanent technical debt without an approved exit criterion.

7 Protect command authority first

Command authority has direct mission and liability consequences. The operator should trace the command path from origin through approval, mission control, networks, ground station, radio link and spacecraft execution. For each stage, identify authentication, encryption, replay protection, sequence control, logging and emergency access.

Migration should be rehearsed on representative systems before a live command path changes. The test plan should cover algorithm negotiation, expired or revoked credentials, link interruption, partial deployment, clock errors, key rollover, corrupted messages, rollback and recovery. Critical commands can require dual control or additional operational gates during transition.

Backup and contingency links deserve equal attention. An emergency path that bypasses modern authentication can become the enduring vulnerability. Where legacy constraints prevent full migration, the operator should bound access, strengthen ground controls, reduce credential exposure and document the residual risk accepted for the remaining mission life.

8 Secure software and firmware updates

Digital signatures protect the software supply chain and the spacecraft update path. Migration affects build systems, code-signing services, hardware roots of trust, bootloaders, deployment packages, verification code and recovery images. A new signature algorithm has limited value when a legacy trust anchor cannot recognise it.

The operator should map every verification step from source commit to running code. The map should identify the signing authority, key custody, build provenance, package format, on-board verification, rollback and recovery. It should also identify long-lived signed artefacts that may need re-signing or dual signatures.

Upgrade sequencing matters. Ground signing infrastructure and reproducible builds should be established before flight verification changes. The operator should retain a known-good recovery route and test it independently. A failed update can destroy more value than the cryptographic risk it was intended to reduce.

9 Evaluate data lifetime and harvest-now exposure

Some satellite data loses value quickly. Other data, including defence, intelligence, infrastructure, scientific or customer information, may remain sensitive for years. An adversary can collect encrypted traffic and decrypt it later if the underlying public-key protection becomes breakable. This creates an economic reason to protect long-lived data before a quantum computer exists.

The inventory should classify data by sensitivity period, exposure path, volume, customer obligation and re-encryption feasibility. The operator should distinguish data in transit, stored archives, mission databases, customer delivery and backups. Symmetric cryptography and key length also need review, even when the principal quantum concern is public-key cryptography.

The capex model should prioritise paths carrying data whose sensitivity outlives the expected migration date. Contract pricing and customer segmentation can reflect the cost of stronger protection where the requirement is service specific.

10 Test performance and resource constraints

Post-quantum algorithms can change key, signature and message sizes and require different computation and memory. The impact must be measured on representative hardware and operational traffic. Desktop benchmarks do not establish flight suitability.

Testing should cover key generation, encapsulation or verification time, peak memory, persistent storage, power, thermal behaviour, bandwidth, packetisation, error rates and interaction with other workloads. The model should include worst-case command windows and contingency modes rather than average laboratory conditions.

Where constraints are material, the operator can evaluate optimised implementations, hardware acceleration, precomputation, protocol changes, ground assistance or a later fleet replacement. Each option changes development cost, qualification, supply risk and residual value.

11 Treat standards readiness as an evidence gate

Final algorithms are a necessary starting point. Deployment also depends on protocol standards, implementation quality, module validation, hardware support, supplier roadmaps and customer accreditation. NIST's migration work and the NCSC timeline recognise that ecosystem maturity develops over several years.

The programme should maintain a readiness register for every dependency. Each line should identify current status, required standard or product, supplier evidence, expected availability, integration lead time and fallback. A procurement announcement should not be treated as delivered capability.

Capex should be released at evidence gates. Discovery and architecture work can begin immediately. Pilot expenditure follows a stable implementation and test environment. Fleet deployment follows performance, safety, interoperability and approval evidence. This sequencing protects cash while preserving schedule.

12 Underwrite supplier and component dependencies

Satellite operators depend on cryptographic libraries, processors, radios, secure elements, hardware security modules, certificate services, ground equipment and specialist engineering. The migration plan should identify which suppliers control each dependency and whether contractual support extends through the intended asset life.

For each critical supplier, review roadmap, validation, licensing, source access, export restrictions, end-of-life policy, change control, vulnerability handling and financial capacity. A supplier's generic PQC roadmap does not prove support for the operator's exact product or configuration.

The operator should budget for second-source qualification or interface abstraction where concentration is material. Procurement terms should require cryptographic inventory, notice of algorithm dependence, support for agreed migration milestones and evidence needed for customer assurance.

13 Construct the capex taxonomy

The programme budget should separate discovery, architecture, laboratories, ground infrastructure, software and firmware, on-board engineering, network and protocol changes, supplier non-recurring engineering, accreditation, customer migration, operations, contingency and replacement assets. This prevents a software estimate from hiding physical and commercial dependencies.

Recurring operating cost should be shown separately from capex. Parallel certificates, dual protocol stacks, additional monitoring, specialist staffing and customer support can continue for years. Financing models should capture the working-capital effect of milestone payments and delayed acceptance.

Every budget line should have a driver. Examples include number of configurations, interfaces, sites, trust domains, customer gateways, qualification campaigns or spacecraft replacements. Driver-based budgeting is more auditable than a percentage of IT expenditure.

14 Sequence capex by option value

Early spending should create information and preserve choices. Inventory, architecture, representative testbeds, supplier commitments and customer engagement reduce uncertainty across the whole programme. They can prevent a new satellite or ground system from entering service with a rigid design.

Irreversible expenditure should follow evidence. Fleet-wide deployment, hardware redesign or accelerated replacement should wait for tested performance, standards maturity and commercial justification. The board should recognise deadlines created by procurement and launch cycles; waiting until a standard is operationally urgent can remove the option to redesign economically.

A useful sequence is discover, design, isolate, pilot, accredit, deploy, retire. Each stage has entry evidence, exit tests, approved spend and a rollback position. The programme can move different fleet segments through the sequence at different speeds.

15 Align migration with satellite life extension

Life extension is attractive when the spacecraft remains reliable and revenue producing. Cryptographic rigidity can shorten the commercially useful life even when propulsion, power and payload remain healthy. Customers or regulators may decline to renew service that cannot meet emerging security requirements.

The asset plan should compare remaining technical life, contracted life, probable renewal, migration cost and replacement timing. A moderate upgrade can preserve value when it extends a high-margin contractable period. The same expenditure can destroy value when an asset is near natural retirement or lacks a reliable update path.

Life-extension decisions should include ground compensation and operational burden. Keeping a legacy asset may require dedicated gateways, manual controls and scarce engineering. Those costs reduce the apparent benefit of deferring replacement.

16 Quantify residual-value risk

Residual value depends on the cash a fleet can generate after the explicit forecast and the market's confidence that the assets remain contractable, maintainable and insurable. A post-quantum gap can reduce renewal probability, increase operating cost, require terminal capex or force earlier retirement.

The valuation model should identify the period in which each asset loses eligibility for material customers or approved algorithms. It should then adjust utilisation, price, margin, capex and retirement value. The change belongs in cash flow and terminal assumptions rather than a single arbitrary cyber discount.

Residual-value risk is concentrated when many satellites share the same rigid design and retirement window. A phased fleet with upgradeable trust anchors can spread capital and preserve options. The model should therefore consider configuration concentration as well as average fleet age.

17 Model contract and accreditation exposure

Customer contracts may contain security standards, change notification, approval, audit, incident, data handling, subcontracting and service-continuity obligations. Migration can require consent or reaccreditation. Failure to migrate can affect renewal, pricing or eligibility.

The operator should map each material contract to affected systems, required standards, approval authority, lead time and revenue at risk. Framework ceilings and announced customer interest remain separate from enforceable revenue. Customer discussions should produce dated evidence rather than general statements of support.

The commercial plan can offer migration tiers, dedicated gateways or accelerated assurance where customers fund the requirement. Any differential service must be operationally separable and accurately described.

18 Incorporate insurance and financing

Insurers and lenders may ask how the operator protects command, software updates, customer data and continuity. The financial model should identify policy conditions, exclusions, disclosure duties, financing covenants and material adverse-change provisions that could be affected by migration gaps or failed deployment.

The operator should avoid claiming quantum-safe status before the end-to-end system supports it. Misstatement can create coverage, disclosure and customer risk. Evidence should identify the protected scope, algorithm, configuration, test and date.

Financing can be aligned with milestones. A capex facility or reserve can fund laboratories, ground upgrades and fleet replacement against documented gates. Lenders can receive reporting on inventory coverage, critical-path tests, customer approvals and remaining exposure without controlling technical decisions.

19 Design the operational transition

Migration must preserve service and positive control. The operator should define coexistence, key rollover, credential issuance, monitoring, incident response, rollback and emergency authority. Procedures should address partial fleet migration and mixed customer endpoints.

Operational rehearsals should use representative command and telemetry flows. Teams should practise failed negotiation, revoked credentials, expired certificates, unavailable key services, corrupted updates and restoration from trusted state. The evidence should include logs, timings, deviations and approved corrective actions.

The transition calendar should avoid critical mission phases where practical. It should also include supplier and customer change freezes. A nominal technical completion date is insufficient when operations cannot demonstrate controlled use.

20 Build the governance and assurance model

The programme needs accountable ownership across engineering, operations, security, finance, procurement, legal and commercial teams. A central programme office should control the inventory, dependencies, budget, evidence gates and exception register. Mission authorities retain responsibility for safety and command decisions.

Independent review is appropriate for critical architecture, cryptographic implementation, update paths and migration exercises. Review should test evidence and assumptions. It should not replace management accountability or customer approval.

Board reporting should show fleet coverage, critical dependencies, milestones, committed and forecast spend, contract exposure, residual-value movement and decisions required. A green programme status should require evidence that the most valuable and constrained assets have viable paths.

21 Construct the hypothetical fleet case

The hypothetical operator has 42 spacecraft. Eighteen are newer, software-defined assets with sufficient resources and tested rollback. Fourteen can accept selected changes but rely on constrained processing and gateway assistance. Ten older assets have fixed or poorly documented trust anchors and limited update capacity. The ground estate includes 11 operational sites, two recovery environments and six customer gateways.

The fleet produces USD 610 million of annual revenue and USD 212 million of EBITDA before migration. Contracted and probability-weighted renewal value is concentrated in the newer and constrained groups. The oldest group contributes USD 72 million of revenue and USD 18 million of EBITDA, with a four-year weighted remaining contract life.

All amounts and probabilities in this case are management assumptions created only to demonstrate the framework. They describe no identified operator, satellite or transaction.

22 Build the illustrative investment programme

The nominal programme totals USD 146 million over seven years. Discovery, architecture and governance require USD 12 million. Testbeds and representative hardware require USD 18 million. Ground PKI, identity, signing and key-management changes require USD 24 million. Link and protocol engineering require USD 20 million. Flight-software work and qualification require USD 31 million. Customer migration and accreditation require USD 16 million. Contingency is USD 25 million.

Evidence weighting classifies USD 82 million as committed or high-confidence because the underlying scope and supplier path are established. USD 39 million remains conditional on performance, protocol and customer gates. USD 25 million is contingency. The model also includes USD 9 million of annual parallel-run cost at peak transition.

The plan retires six older spacecraft at natural contract expiry, harvests four under bounded controls and prioritises the highest-value newer assets for migration. This avoids spending the same amount on every spacecraft.

23 Compare timing scenarios

The accelerated case completes high-priority ground and software-signing changes in two years, migrates the newer flight group by year four and completes the economically justified fleet by year six. It has the highest near-term spend and the lowest contract-renewal exposure.

The base case uses a seven-year programme. It aligns deployments with planned software releases and customer accreditation. The delayed case begins fleet engineering three years later. It preserves near-term cash but compresses procurement, qualification and replacement into a shorter window.

Under the illustrative assumptions, the delayed case reduces residual value by USD 238 million relative to the base case. The reduction reflects lower renewal probability, higher terminal capex, concentrated retirements and weaker terminal growth. The model does not assume a quantum attack.

24 Stress the economics

The principal sensitivities are implementation maturity, customer deadlines, replacement lead time, on-board performance, supplier concentration and the remaining life of constrained spacecraft. The downside case increases programme cost by 30%, delays customer acceptance by two years and forces replacement of four additional spacecraft.

The severe case combines a failed on-board pilot, a supplier end-of-life notice and earlier security requirements from two major customers. It produces a temporary capacity shortfall and requires accelerated launches. The board should test liquidity through this combined case because technical and commercial risks can be correlated.

The investment remains rational when funded migration preserves discounted contract contribution greater than programme and operating cost. Assets that fail that test move to harvest, compensate or retire.

25 Translate the framework into a mandate

A fleet-modernisation mandate should begin with a verified configuration and cryptographic inventory, a customer and regulatory map, and a decision model that connects each technical path to cash. The adviser should coordinate engineering, cyber, commercial, legal, insurance and financing workstreams around one evidence register.

Stage gates should approve discovery, target architecture, representative pilots, customer accreditation, fleet deployment and retirement. Each gate should state the accepted evidence, remaining risk, spend released and effect on residual value. Exceptions should identify the customer, mission, duration, compensating control and accountable executive.

The financing workstream should compare operating cash, asset-level debt, capex facilities, customer contributions and strategic funding. The structure should match the useful life and cash benefit of the expenditure. Short-lived legacy compensation should not be financed as though it creates a long-lived asset.

26 Embed requirements in procurement and new missions

The cheapest migration is the dependency that does not enter the next design. New spacecraft, payloads and ground systems should therefore include explicit requirements for algorithm replacement, maintained cryptographic inventory, bounded interfaces, secure update, rollback, key custody, telemetry and supplier support. Acceptance should test those properties on the delivered configuration. A promise that a product is quantum ready has limited value without an identified standard, implementation, resource profile and operational test.

Procurement should also distinguish deliverables from options. The supplier can provide a validated implementation, test vectors, source or escrow rights, migration documentation, performance evidence and notice of end of life. An option to add post-quantum support later should state price, schedule, dependencies and acceptance. The operator should avoid paying a premium for an undefined future capability.

Fleet commonality creates purchasing leverage and correlated risk. A common cryptographic module can reduce integration cost across configurations, while one defect or supplier withdrawal can affect the full fleet. The procurement case should therefore measure the benefit of commonality alongside the cost and readiness of a second implementation or replaceable interface.

27 Coordinate replacement launches and capacity

Some legacy spacecraft will fail the migration economics and require replacement. The replacement plan should include satellite manufacture, launch procurement, licensing, orbital deployment, customer transition and decommissioning. Cryptographic capex cannot be evaluated separately from this capacity path because a late replacement can force the operator to retain a weak asset or lose service.

The operator should model replacement batches by mission value and design concentration. Replacing every legacy asset in one design generation can recreate a common retirement cliff. Phased procurement can incorporate improving standards and operational evidence, provided the fleet retains interoperable ground services and sufficient scale.

Launch and manufacturing capacity should be evidenced through binding commitments and realistic integration schedules. Frameworks and supplier forecasts remain scenario inputs until capacity, price and delivery obligations are enforceable. The liquidity model should include deposits, construction milestones, insurance, launch payments and delayed customer activation.

The residual-value comparison should include the option value of delaying selected replacements after a successful compensated-control period. It should also include the cost of keeping specialised gateways, staff and spares. This makes the harvest decision explicit and prevents deferral from appearing free.

28 Establish the residual-value accounting bridge

The investment committee should reconcile technical findings to the asset register and valuation model. The starting point is the carrying or enterprise value assigned to each fleet cohort. The model then identifies forecast cash that depends on quantum-vulnerable cryptography, the expenditure required to preserve that cash, the probability and timing of customer acceptance, and the replacement or retirement cash flows that remain after the explicit forecast.

The bridge should avoid double counting. A lower renewal probability and an additional terminal-capex deduction can represent the same exposure when the customer departure is caused by the unavailable upgrade. Engineering should describe the technical consequence; commercial teams should identify affected revenue; finance should convert the supported consequence into one model adjustment. The evidence register should show that lineage.

Accounting useful life and economic useful life can diverge. A spacecraft may continue operating safely while its addressable customer set narrows. A ground asset may be physically sound but require replacement because its cryptographic module cannot be validated or supported. Management should review impairment indicators and disclosure obligations with its accounting advisers using current facts and applicable standards.

The decision model should also preserve upside. A tested, agile configuration can support new secure-services revenue, longer contracts or lower assurance cost. These benefits should enter the case only when customer demand, pricing and delivery capacity are evidenced. A general claim of strategic importance should remain outside base cash flow.

29 Prepare customer and regulator evidence packs

Migration credibility depends on evidence that another party can evaluate. The operator should prepare a configuration-specific pack containing scope, architecture, standards, validated components,

implementation records, performance results, security tests, operational rehearsal, residual exceptions and the approved transition schedule. Sensitive details can be controlled through appropriate access and confidentiality.

The pack should distinguish algorithm compliance from end-to-end service assurance. A FIPS-standard algorithm does not prove that key generation, implementation, protocol integration, update handling or operational custody is correct. Customers need to understand which path is protected, which legacy component remains, and which compensating control applies.

Evidence packs can be reused across customers when the configuration and requirements are common. Customer-specific annexes should cover interfaces, data lifetime, service levels, approval and incident notification. This reduces repeated assurance cost and gives management a clearer view of which revenue depends on unresolved work.

Regulator and government engagement should begin early for high-consequence systems. The operator should record guidance, submissions, questions, responses and approval assumptions. Informal discussions can inform planning; only formal requirements and decisions should be treated as binding evidence in the investment case.

Conclusion

Post-quantum migration is a fleet investment problem with security, operational and contractual dimensions. Standards and national roadmaps create urgency, while satellite lifecycles and mission safety require disciplined sequencing. The operator creates value by discovering dependencies early, designing changeable architectures, testing representative systems and directing capital toward assets with supported contract life.

The board should evaluate each configuration through migrate, compensate or retire. Capex should follow evidence gates and customer value. Residual value should reflect contractability, terminal capital and concentration of rigid designs. This approach allows the fleet to transition without converting uncertain quantum timing into either complacency or indiscriminate expenditure.

Appendix A Fleet evidence register

For every spacecraft and ground configuration, record owner, mission, launch date, expected retirement, contracted service, processor, memory, secure boot, update path, rollback, cryptographic library, algorithms, protocols, trust anchors, key custody, signing chain, customer interface, supplier, test environment, approval authority and current evidence date.

For every unresolved dependency, record consequence, planned test, budget, decision date and fallback. Preserve contradictory evidence and identify which valuation or capex line it affects.

Appendix B Investment case checklist

Reconcile the fleet inventory to contracts, asset register, insurance schedule, financing security and operational configuration. Build capex by driver and phase. Separate recurring cost, parallel-run cost, replacement assets and contingency. Link each spend line to a measurable completion event.

Calculate residual value by fleet cohort. Show renewal probability, margin, remaining life, terminal capex and retirement cost. Stress customer deadlines, supplier delay, implementation performance and launch replacement capacity.

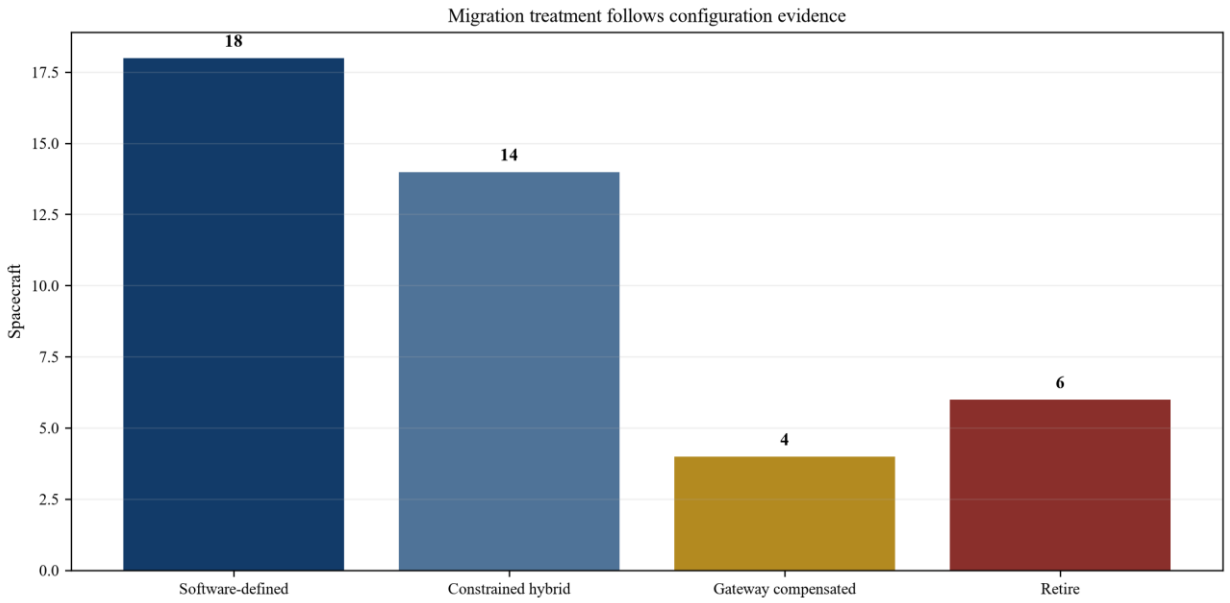
Appendix C Governance checklist

Approve a target architecture, algorithm policy, transition sequence, exception process, assurance plan, customer communication and reporting cadence. Maintain configuration control and a full decision record. Require operational rehearsal before live migration of command or update paths.

Report inventory coverage, critical-path maturity, committed spend, forecast spend, customer approvals, residual-value movement, incidents and exceptions. Return to the board when a critical supplier, standard, customer deadline or replacement assumption changes materially.

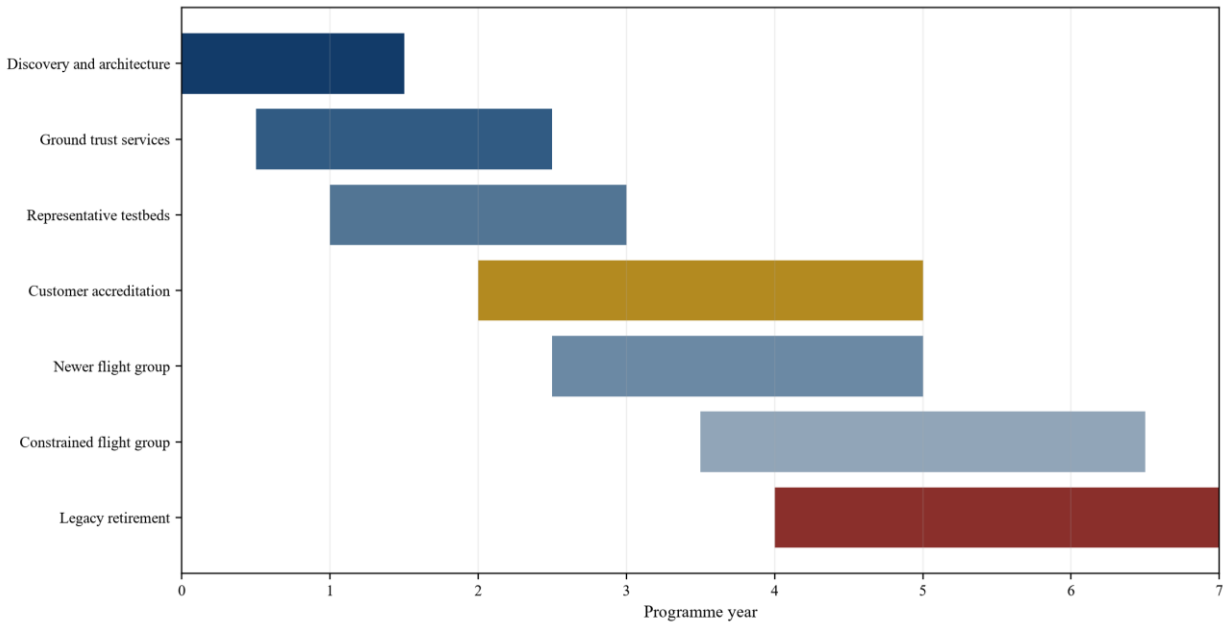
Appendix D Decision figures and tables

Figure 1. Fleet cryptographic exposure map



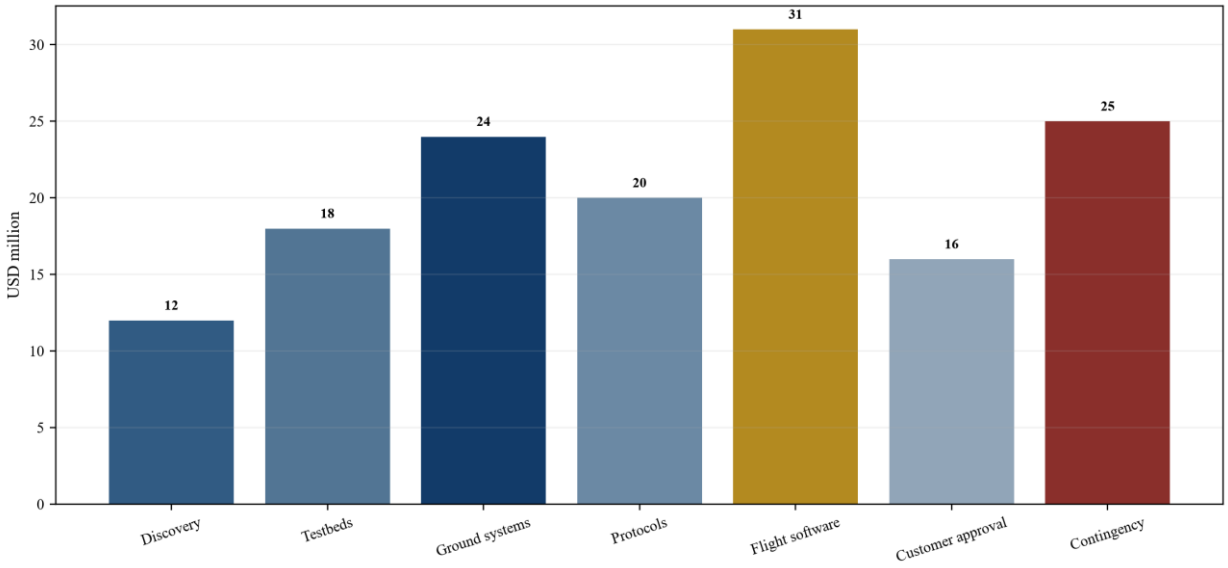
Wholly hypothetical; counts represent spacecraft configurations.

Figure 2. Illustrative seven-year migration schedule



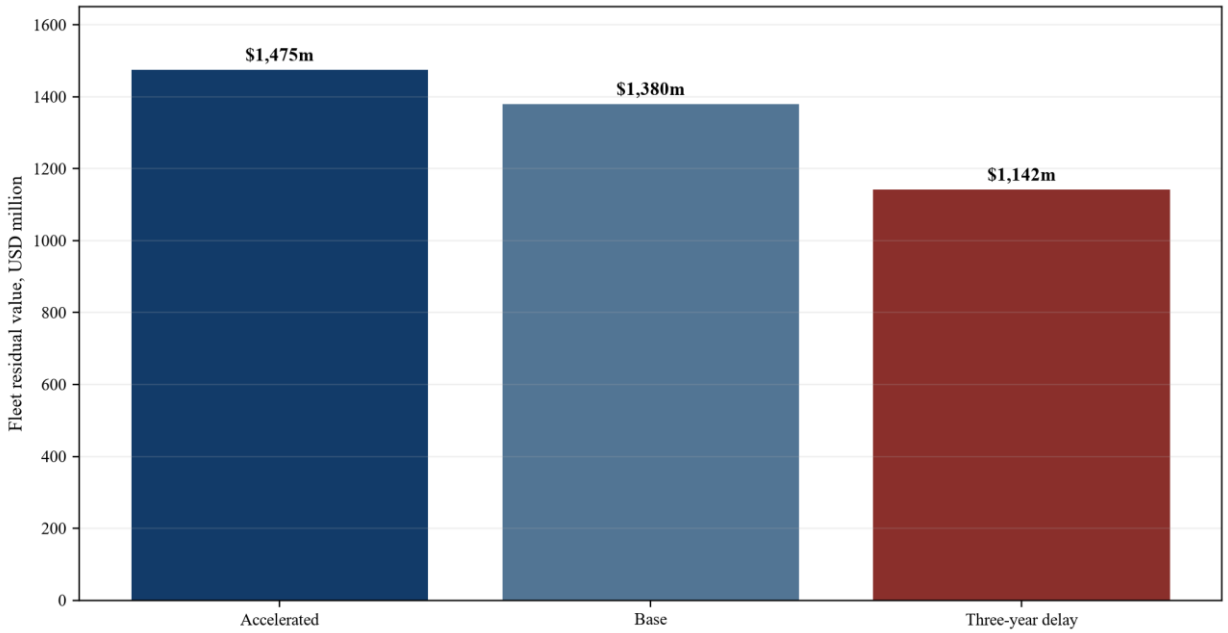
Hypothetical sequencing; timing depends on standards, suppliers and mission windows.

Figure 3. Illustrative nominal capex by workstream



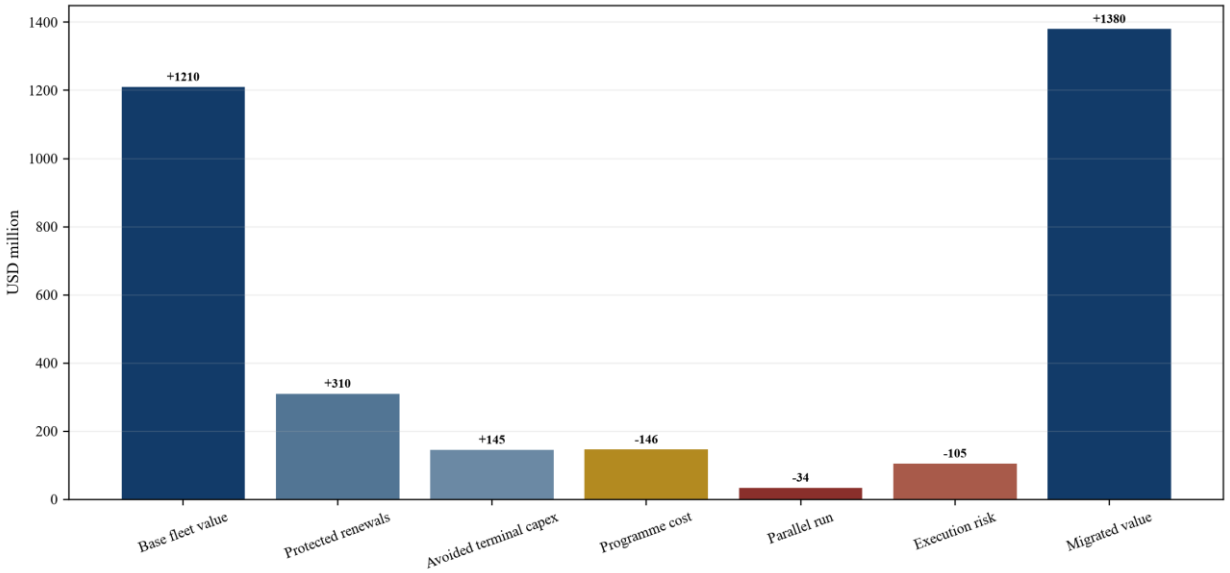
Wholly hypothetical; USD million.

Figure 4. Residual value under migration timing scenarios



Wholly hypothetical; USD million at the valuation date.

Figure 5. Illustrative migration value bridge



Wholly hypothetical; USD million present value.

Table 1. Cryptographic discovery fields

Domain	Required evidence	Principal decision	Economic consequence
Command	Algorithm, keys, sequence and recovery	Migrate or compensate	Mission continuity and liability
Software signing	Trust anchor, build and rollback	Replace, dual sign or retire	Update eligibility and engineering cost
Ground identity	Directories, certificates and privilege	Routine migration path	Operating capex and assurance
Customer interface	Protocol, contract and approval	Sequence by customer	Renewal probability and price
Stored data	Sensitivity period and re-encryption	Prioritise long-lived data	Contract and disclosure exposure
Supplier component	Product, version and roadmap	Qualify, abstract or replace	Schedule and concentration risk

Proposed minimum fleet inventory.

Table 2. Fleet migration archetypes

Archetype	Technical evidence	Primary treatment	Residual-value effect
Software defined	Resources, modular crypto and tested rollback	Direct migration	Preserves longer contractable life
Constrained hybrid	Limited resources and bounded update path	Optimised or hybrid migration	Value depends on test and approval
Gateway compensated	Rigid on-board implementation	Ground control and reduced exposure	Shorter renewal horizon
Harvest or retire	No acceptable protected path	Run off or replace	Earlier retirement and replacement capex

Proposed classification; evidence should be configuration specific.

Table 3. Illustrative programme budget

Workstream	High-confidence	Conditional	Contingency	Total
Discovery and architecture	12	0	0	12
Testbeds and representative hardware	11	7	0	18
Ground trust services	21	3	0	24
Link and protocol engineering	10	10	0	20
Flight software and qualification	18	13	0	31
Customer migration and accreditation	10	6	0	16
Programme contingency	0	0	25	25
Total	82	39	25	146

Wholly hypothetical; USD million.

Table 4. Capex release gates

Gate	Required evidence	Spend released	Board question
Discovery	Maintained inventory and consequence map	Architecture and testbed	Is the perimeter complete?
Architecture	Target profiles and supplier dependencies	Representative pilots	Is the end state changeable?
Pilot	Performance, rollback and safety tests	Customer accreditation	Can the configuration operate safely?
Accreditation	Written customer and authority path	Fleet deployment	Is revenue protected?
Deployment	Operational rehearsal and accepted evidence	Scale rollout	Can mixed-fleet operation be controlled?
Retirement	Contract, replacement and decommissioning plan	Replacement capital	Is further migration value creating?

Proposed governance sequence.

Table 5. Illustrative timing scenarios

Scenario	Programme duration	Nominal spend	Residual value	Principal exposure
Accelerated	6 years	164	1475	Higher near-term execution load
Base	7 years	146	1380	Balanced standards and renewal timing
Three-year delay	7 years after deferral	172	1142	Compressed replacement and lost renewals

Wholly hypothetical.

Table 6. Contract and financing workstream

Exposure	Evidence	Model treatment	Control
Security requirement	Contract and customer standard	Renewal and capex timing	Written acceptance path
Change approval	Consent and accreditation lead time	Delay and working capital	Stage-gated deployment
Insurance	Policy, condition and disclosure	Premium and coverage scenario	Accurate scope statement
Financing	Covenant, reserve and asset security	Liquidity and funding cost	Milestone reporting
Supplier roadmap	Contract, validation and end-of-life	Schedule and contingency	Second source or abstraction
Retirement	Service exit and decommissioning	Terminal capex and cash	Funded replacement plan

Proposed review; applicable law and contractual terms require specialist advice.

Table 7. Board dashboard

Measure	Evidence	Threshold question	Decision
Inventory coverage	Configurations reconciled to assets	Are critical dependencies known?	Continue discovery or release design spend
Pilot readiness	Representative hardware and protocols	Is performance proven?	Release accreditation spend
Customer coverage	Revenue with documented path	Are renewals protected?	Reprioritise fleet sequence
Spend confidence	Committed, conditional and contingency	Is liquidity adequate?	Fund, phase or redesign
Residual value	Cohort cash flow and terminal capex	Has migration preserved asset life?	Migrate, compensate or retire
Operational evidence	Exercises, logs and rollback	Can transition be controlled?	Approve deployment

Proposed recurring measures.

Frequently asked questions

Q: Does a satellite operator need to know when a cryptographically relevant quantum computer will exist? A: No precise arrival date is required for planning. The operator should compare data lifetime, asset life, procurement lead time, accreditation time and the dates by which customers or authorities expect migration. These factors can create an investment deadline before a quantum computer exists.

Q: Should every spacecraft receive the same post-quantum upgrade? A: No. The operator should classify each configuration by technical capability, remaining contract life, mission consequence and migration economics. Some assets justify direct migration, some require compensating controls, and some should be harvested or retired.

Q: What should be funded first? A: Cryptographic discovery, target architecture, representative testbeds, supplier commitments and customer engagement create information and preserve options. Fleet-wide deployment should follow performance, safety, interoperability and accreditation evidence.

Q: Can ground gateways solve the problem for legacy spacecraft? A: Gateways can reduce exposure and provide compensating controls for selected functions. They cannot automatically replace an immutable

on-board trust anchor, weak command authentication or an update verifier that depends solely on quantum-vulnerable cryptography. The protected scope must be stated precisely.

Q: How should hybrid classical and post-quantum mechanisms be valued? A: The operator should test the exact protocol, performance and failure behaviour and define when classical dependence ends. Value follows accepted operation and preserved customer eligibility rather than the presence of two algorithms.

Q: How does migration affect residual value? A: Migration can preserve renewal probability, operating margin and contractable life. Delay can increase terminal capex, compress replacements and shorten the period in which legacy assets remain eligible. These effects should be modelled in cash flow and terminal assumptions.

Q: What evidence should lenders and insurers receive? A: Useful evidence includes inventory coverage, target architecture, critical-path dependencies, validated implementations, representative tests, customer approval paths, operational exercises, funded capex and unresolved exceptions. Claims should identify the exact protected scope and configuration.

Q: When should a legacy satellite be retired rather than upgraded? A: Retirement is appropriate when the cost and operational risk of migration exceed the supported contract contribution and option value preserved. The comparison should include gateway burden, customer renewal, replacement lead time, decommissioning and mission capacity.

References

[1] National Institute of Standards and Technology, Post-Quantum Cryptography Project. https://csrc.nist.gov/projects/post-quantum-cryptography

[2] National Institute of Standards and Technology, FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024. https://csrc.nist.gov/pubs/fips/203/final

[3] National Institute of Standards and Technology, FIPS 204 Module-Lattice-Based Digital Signature Standard, 2024. https://csrc.nist.gov/pubs/fips/204/final

[4] National Institute of Standards and Technology, FIPS 205 Stateless Hash-Based Digital Signature Standard, 2024. https://csrc.nist.gov/pubs/fips/205/final

[5] National Institute of Standards and Technology, NIST IR 8547 Transition to Post-Quantum Cryptography Standards. https://csrc.nist.gov/pubs/ir/8547/ipd

[6] National Cybersecurity Center of Excellence, Migration to Post-Quantum Cryptography. https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/

[7] National Institute of Standards and Technology, Cybersecurity White Paper 39 Considerations for Achieving Crypto Agility, 2025. https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-crypto-agility/final

[8] National Institute of Standards and Technology, SP 800-227 Recommendations for Key-Encapsulation Mechanisms, 2025. https://csrc.nist.gov/pubs/sp/800/227/final

[9] National Institute of Standards and Technology, SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes, 2020. https://csrc.nist.gov/pubs/sp/800/208/final

[10] National Institute of Standards and Technology, Cryptographic Module Validation Program. https://csrc.nist.gov/projects/cryptographic-module-validation-program

[11] Cybersecurity and Infrastructure Security Agency, National Security Agency and NIST, Quantum-Readiness: Migration to Post-Quantum Cryptography, 2023. https://www.cisa.gov/sites/default/files/2023-08/Quantum-Readiness%20-%20Migration%20to%20Post-Quantum%20Cryptography_508c.pdf

[12] United States Office of Management and Budget, M-23-02 Migrating to Post-Quantum Cryptography, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[13] National Security Agency, Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[14] United Kingdom National Cyber Security Centre, Timelines for Migration to Post-Quantum Cryptography, 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[15] European Commission, Post-Quantum Cryptography Policy and Coordinated Implementation Roadmap. https://digital-strategy.ec.europa.eu/en/policies/post-quantum-cryptography

[16] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 2025. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[17] National Aeronautics and Space Administration, NASA-STD-1006A Space System Protection Standard. https://standards.nasa.gov/node/2430

[18] National Aeronautics and Space Administration, Ground Data Systems and Mission Operations, State of the Art Report, 2026. https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations/

[19] National Aeronautics and Space Administration, Space Security Best Practices Guide. https://www.nasa.gov/general/nasa-issues-new-space-security-best-practices-guide/

[20] National Aeronautics and Space Administration, Software Engineering Handbook SWE-157 Protect Against Unauthorized Access. https://swehb.nasa.gov/spaces/SWEHBVD/pages/102695513/SWE-157%2B-%2BProtect%2BAgainst%2BUnauthorized%2BAccess

[21] National Aeronautics and Space Administration, Software-Only Key Management and Cryptography for Spacecraft Command Encryption, 2023. https://ntrs.nasa.gov/citations/20230001612

[22] National Aeronautics and Space Administration, Bulk Security Standard for Spacecraft Communication GSFC-STD-8012A, 2026. https://standards.nasa.gov/node/12195

[23] Consultative Committee for Space Data Systems, CCSDS 355.0-B-2 Space Data Link Security Protocol, 2022. https://ccsds.org/view/bluebooks/entry/3258/

[24] Consultative Committee for Space Data Systems, Security Working Group Publications. https://public.ccsds.org/Publications/Security.aspx

[25] European Union Agency for Cybersecurity, ENISA Space Threat Landscape 2025. https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025

[26] European Union Agency for Cybersecurity, Low Earth Orbit SATCOM Cybersecurity Assessment, 2024. https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment

[27] European Space Agency, ACES Advanced Cryptography and Secured by Design for 5G and 6G Satellite Communications, 2026. https://resilience.esa.int/archives/projects/aces

[28] European Space Agency, Eagle-1. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1

[29] European Space Agency, QKDSat Secure Communication via Quantum Cryptography. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/QKDSat_Secure_communication_via_quantum_cryptography

[30] United States Office of Space Commerce, Space Policy Directive 5 Cybersecurity Principles for Space Systems. https://space.commerce.gov/president-signs-space-cybersecurity-policy-directive/

[31] National Institute of Standards and Technology, NISTIR 8401 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control. https://csrc.nist.gov/pubs/ir/8401/final

[32] National Institute of Standards and Technology, SP 800-218 Secure Software Development Framework Version 1.1. https://csrc.nist.gov/pubs/sp/800/218/final

[33] National Institute of Standards and Technology, Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

[34] European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

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.