Factors to Consider When Preparing a Budget for PQC Migration

Q-Prep conducted an in-depth interview with **Raj Chanian**, Post-Quantum Cryptography (PQC) Lead Solutions Architect at Capgemini, to capture expert insights on the financial and operational considerations of PQC migration.

Drawing on his experience, supporting highly regulated organisations, Raj provides a pragmatic, delivery-focused view on how institutions should approach PQC budgeting. His insights emphasise risk-based prioritisation, early discovery, crypto-agility, and alignment with broader modernisation initiatives—helping organisations understand not just *what* PQC migration costs, but *why*, *when*, and *how* those costs can be effectively managed.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Interview Questions

1 Are there cost models per industry sector or type of public institution?

NIST IR 8547

This recommends considering multiple impact factors when budgeting for PQC migration. These include inventory complexity, system criticality for high-value or long-lived data, vendor readiness for updates and support, and interoperability during hybrid deployments. Additional factors involve testing for performance and security, stakeholder coordination, and ongoing compliance monitoring. Rather than fixed cost estimates, NIST advises a phased, activity-based approach—discovery, planning, implementation, validation, and monitoring. This enables risk-based prioritisation, efficient resource allocation, and adaptability to evolving standards, ensuring secure and cost-effective PQC.

ASC X9 Financial Readiness Needs Assessment

This guides PQC migration budgeting through risk-based prioritisation and crypto-agility. It highlights factors such as cryptographic inventory size, system criticality, and vendor dependencies for PQC support. Recommended actions include allocating resources for discovery, planning, and testing, while accounting for hybrid deployments and compliance costs. The report urges integrating PQC migration into modernisation initiatives to reduce long-term expenses. Early vendor engagement and phased implementation are emphasised as strategies to manage costs effectively and mitigate future operational risks.

MITRE PQC Migration Roadmap

This outlines cost guidance through four phases: Preparation, Baseline Understanding, Planning & Execution, and Monitoring. It emphasises impact factors such as cryptographic asset inventories, system interdependencies, and vendor readiness. Early budgeting should include discovery tools, risk assessments, and stakeholder engagement to establish a strong foundation. During implementation, costs for testing PQC algorithms, hybrid deployments, and performance validation are critical. MITRE advises integrating migration into broader modernisation initiatives and securing funding through strategic communication. Continuous monitoring and maintaining crypto-agility are highlighted as ongoing expenses to ensure resilience, adaptability, and compliance throughout the transition. This phased approach enables organisations to manage costs effectively while mitigating operational and security risks associated with PQC.

ETSI TR 103 619 Migration Strategies Report

This offers cost guidance through a structured approach comprising diagnosis, planning, and execution phases. It identifies key impact factors such as cryptographic asset inventories, system dependencies, and vendor readiness for PQC support. Budgeting should incorporate expenses for risk assessments, hybrid deployments, and performance testing to guarantee interoperability and security. ETSI stresses early investment in crypto-agility and phased implementation to minimise disruption and reduce long-term costs. Additional recommendations include allocating resources for workforce training, compliance

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

activities, and continuous monitoring to maintain resilience. The strategy emphasises aligning technical migration with broader business objectives, ensuring cost efficiency while mitigating operational and regulatory risks. By adopting this structured roadmap, organisations can manage PQC migration effectively, balancing upfront investments with ongoing operational needs for sustainable cryptographic transformation.

PQC Migration Handbook by AIVD, CWI, and TNO

This provides practical budgeting guidance for PQC migration, emphasising early preparation and crypto-agility. It identifies critical impact factors such as cryptographic asset inventories, system dependencies, and vendor readiness, while advocating risk-based prioritisation to optimise resource allocation. A key concept introduced is No-Regret Moves—proactive steps like conducting comprehensive inventories and adopting crypto-agile architectures early to reduce future costs and complexity. Budgeting should account for testing, compliance, and workforce training, alongside resources for hybrid deployments during transitional phases. The handbook underscores continuous monitoring and adaptability as essential for managing long-term operational expenses and maintaining resilience against evolving cryptographic threats. By integrating PQC migration into broader modernisation strategies and securing stakeholder engagement, organisations can achieve cost efficiency, regulatory compliance, and sustained cryptographic agility throughout the transition.

FS-ISAC Roadmap for the Financial Sector

This outlines cost guidance through a four-phase migration model: Initiation, Discovery, Deployment, and Exit. It emphasises impact factors such as cryptographic asset inventories, system criticality, and vendor readiness for PQC support. Budgeting should include expenses for inventory automation, risk assessments, and hybrid deployments during transitional stages. The roadmap warns against "crypto-procrastination," noting that delays can lead to higher costs and operational risks. It recommends allocating resources for testing, training, and regulatory compliance while integrating PQC migration into broader modernisation initiatives. This approach optimises cost efficiency, strengthens resilience, and ensures readiness against emerging quantum threats. By adopting a phased strategy and engaging stakeholders early, organisations can manage financial impacts effectively and maintain long-term.

The FS-ISAC Roadmap is highly relevant to regulatory compliance in the FS sector because it aligns PQC migration with key regulatory expectations around risk management, operational resilience, and data protection, so we can take this lens from the following perspective

Regulatory Mandates for Cryptographic Security

Financial regulators (e.g., FFIEC, EBA, and regional authorities) require institutions to maintain strong encryption for sensitive data. The roadmap's emphasis on cryptographic asset inventories and system criticality ensures compliance with these mandates by identifying and prioritising high-risk systems that handle regulated financial data.

Risk-Based Approach

Regulations often demand risk-based planning for technology transitions. FS-ISAC's phased model—Initiation, Discovery, Deployment, Exit—supports this by enabling structured migration, reducing systemic risk, and avoiding abrupt changes that could violate operational continuity requirements.

Compliance and Audit Readiness

The roadmap explicitly calls for budgeting resources for testing, training, and regulatory compliance, which aligns with audit requirements under frameworks like PCI DSS, SOX, and GDPR. Continuous monitoring and documentation during migration help demonstrate adherence to regulatory standards.

Avoiding Operational Risk

"Crypto procrastination" warnings reflect regulatory concerns about delayed adoption of secure cryptographic standards. Regulators expect proactive measures to mitigate emerging quantum threats, and early engagement reduces exposure to compliance penalties and reputational damage.

Integration with Modernisation

Regulators encourage modernisation strategies that enhance resilience. FS-ISAC's recommendation to integrate PQC migration into broader modernisation efforts ensures alignment with supervisory guidance on technology risk management and future-proofing critical infrastructure.

The CISA Strategy for Automated PQC Discovery emphasises cost reduction through automation and seamless integration with existing security frameworks. It identifies critical impact factors such as cryptographic asset visibility, tooling requirements, and operational complexity. Budget planning should prioritise investments in automated discovery solutions, continuous diagnostics, and integration with programs like Continuous Diagnostics and Mitigation to enhance efficiency. This automation-driven approach significantly reduces manual inventory costs, accelerates risk assessments, and improves accuracy. Additional considerations include vendor coordination for PQC readiness, algorithm testing, and ongoing compliance monitoring to meet regulatory standards. CISA strongly advocates early adoption of automation to streamline migration processes, minimise labour expenses, and ensure scalability for large, complex environments. By embedding automation into PQC migration strategies, organisations can achieve faster implementation, maintain operational resilience, and reduce long-term costs while preparing for emerging quantum threats.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2 What factors are the most significant in influencing the cost?

Timeline Perspective of Initiating PQC Readiness Engagement

The timing of PQC readiness engagement greatly influences overall migration costs. Starting early enables proactive planning, phased implementation, and efficient resource allocation, reducing last-minute changes and operational disruptions. It allows organisations to leverage existing budgets, avoid premium charges for urgent vendor support, and minimise accelerated timeline risks.

Conversely, a delayed start compresses schedules, driving up labour, tooling, and consulting costs due to expedited work and potential rework from insufficient preparation. Early engagement also fosters stakeholder alignment and dependency management, mitigating hidden expenses. In essence, initiating PQC readiness early ensures predictability and cost efficiency, while late engagement escalates financial and operational risks significantly.

Tooling Perspective

The decision between using in-house tools and procuring external solutions for PQC migration has a significant impact on overall costs. In-house tools can reduce licensing fees and offer greater customisation, aligning closely with organisational requirements. However, they demand internal development, ongoing maintenance, and skilled resources, which can increase labour costs and extend project timelines.

Conversely, external solutions provide faster deployment, vendor expertise, and proven reliability, but involve upfront purchase costs, subscription fees, and integration expenses. These tools often accelerate compliance and reduce risk, helping avoid costly delays or rework. Ultimately, the choice affects budget predictability, scalability, and long-term operational expenses. Careful evaluation of technical capability, resource availability, and risk tolerance is essential to determine the most cost-effective and sustainable approach for PQC migration.

Cryptography Inventory Perspective

The accuracy, completeness, and quality of an enterprise cryptographic inventory play a pivotal role in determining PQC migration costs. A well-structured and detailed inventory enables precise scoping, reducing uncertainty and preventing resource overestimation or underestimation. High-quality data accelerates planning, minimises discovery efforts, and avoids costly surprises such as overlooked algorithms or hidden system dependencies.

Conversely, incomplete or poor-quality inventories lead to rework, extended timelines, and emergency fixes, significantly increasing labour and consulting expenses. Comprehensive inventories also support effective risk prioritisation and phased migration strategies, ensuring optimal budget allocation and reducing operational disruption. In short, investing in a robust inventory upfront lowers hidden costs, improves predictability, and enhances migration efficiency, while gaps or inaccuracies can dramatically inflate total expenses and undermine project success.

Skills Capability Maturity Perspective

An organisation's skills capability maturity has a profound impact on PQC migration costs. High maturity—where internal teams possess advanced expertise in cryptography, security architecture, and PQC standards—significantly reduces reliance on costly external suppliers, consultants, and systems integrators. Skilled teams can manage complex dependencies, optimise tool usage, and streamline integration processes internally, accelerating planning and minimising errors. This capability not only lowers overall costs but also enhances agility and decision-making quality throughout the migration lifecycle.

Conversely, low maturity introduces substantial challenges. Organisations lacking PQC expertise face increased training requirements and heavy dependence on third-party services, which often come at premium rates. These gaps heighten the risk of misconfigurations, inefficient solutions, and compliance failures, leading to delays, rework, and inflated budgets. Poor decision-making driven by limited knowledge can further compound costs by selecting suboptimal strategies or tools. In short, mature internal capabilities enable cost efficiency, predictability, and resilience, while low maturity escalates expenses and operational risks dramatically. Investing in skill development early is critical for sustainable, secure, and cost-effective PQC migration.

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

3 Do outsourced IT managed services make a difference to the cost of migration?

Service Offerings Perspective

IT managed services play a critical role in shaping PQC migration costs through their scope, delivery models, and level of expertise. Comprehensive managed service offerings can significantly reduce internal resource strain by providing end-to-end support, including migration planning, implementation, and ongoing maintenance. These services often bundle monitoring, compliance management, and lifecycle oversight, which improves predictability, mitigates risk, and minimises hidden costs. By leveraging specialised expertise, organisations can accelerate migration timelines and avoid costly delays or misconfigurations. However, extensive service packages typically involve higher upfront expenditures compared to selective outsourcing or in-house approaches.

Conversely, limited managed service offerings may create gaps that require additional vendors or internal effort, inflating overall costs and complicating coordination. The flexibility, scalability, and maturity of the managed service provider directly influence budgeting accuracy and long-term cost efficiency. Organisations must carefully evaluate service scope, contractual terms, and integration capabilities to ensure alignment with PQC migration objectives. In short, well-structured managed services can optimise cost and resilience, while inadequate coverage increases complexity and financial risk.

Systems Integration Capability Perspective

IT managed services combined with strong systems integration capabilities have a profound impact on PQC migration costs and overall success. Managed services that include robust integration expertise can streamline deployment across complex, multi-vendor environments, reducing delays, minimising rework, and eliminating hidden costs. High integration maturity ensures seamless interoperability between legacy systems, newly implemented PQC solutions, and third-party tools, which significantly lowers customisation requirements and testing overhead. This alignment accelerates migration timelines and enhances predictability, enabling organisations to maintain operational continuity while meeting compliance objectives.

Conversely, weak integration capability creates fragmented processes, leading to higher consulting fees, extended timelines, and increased risk of misconfigurations. These inefficiencies inflate total migration costs and introduce budget unpredictability. Managed services offering end-to-end integration reduce complexity, mitigate risk, and provide a single point of accountability, whereas siloed or limited capabilities often require additional vendors and coordination efforts, compounding expenses.

Integration strength is a critical cost driver for PQC migration. Organisations should prioritise managed service providers with proven integration maturity, flexible delivery models, and experience in cryptographic modernisation. Doing so ensures cost efficiency,

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

scalability, and resilience, while poor integration planning can result in significant financial and operational setbacks.

Quality Assurance QA Perspective

IT managed services and robust QA capabilities exert a decisive influence on PQC migration costs. When the service provider applies disciplined QA practices - covering test strategy, automated regression, compliance validation - defects surface early, interfaces stabilise, and non-functional risks are quantified before production. That rigor reduces rollbacks and rework, accelerates defect isolation, and improves reliability, lowering long-term operational cost and overall disruption.

High QA maturity also brings repeatable processes: fit-for-purpose test environments, data management, secure configuration baselines, and clear exit criteria. These reduce integration uncertainty across legacy systems, cryptographic libraries, and hardware security modules, helping teams hit migration windows with predictable outcomes and tighter cost control. Strong QA baked into managed services further enables risk-based testing aligned to business criticality, so testing effort is focused where failure would be most costly.

Conversely, weak QA capability tends to overlook vulnerabilities, delay issue triage, and miss performance bottlenecks or compliance gaps. The result is elongated timelines, unplanned remediation, and heightened exposure to security findings, all of which inflate total migration budgets. Hidden risks surface late - during user acceptance or production rollout - driving emergency workstreams, change freezes, and reputational impact.

Comprehensive QA embedded within managed services delivers measurable cost efficiency for PQC migration by preventing defects instead of paying for them later. Inadequate QA, by contrast, shifts cost to the right through rework, incident response, and operational instability. Investing in mature QA - people, process, and automation - reduces uncertainty, increases confidence in cryptographic change, and provides a safer, more economical path to PQC readiness.

Offloading Risk Perspective

IT managed services combined with risk offloading play a critical role in controlling PQC migration costs. When providers assume responsibilities for compliance, security, and operational continuity, organisations reduce exposure to unforeseen issues such as penalties, downtime, and emergency remediation. Transferring risk to managed service partners creates predictable pricing models and alleviates internal resource strain, enabling smoother migration execution.

High levels of risk offloading shift liability to providers, ensuring contractual safeguards and cost stability. This approach minimises the financial impact of migration failures and supports business resilience during cryptographic transitions.

Conversely, limited risk transfer leaves organisations vulnerable to integration errors, compliance gaps, and operational disruptions. These exposures often lead to increased insurance premiums, contingency budgets, and recovery expenses, significantly inflating overall migration costs. Unaddressed risks can surface late in the process, triggering emergency fixes and reputational damage.

Comprehensive risk management embedded within managed services mitigates hidden vulnerabilities and delivers predictable outcomes. Inadequate coverage, however, introduces uncertainty and cost volatility. Investing in robust risk-sharing frameworks ensures financial control, operational continuity, and a safer, more economical path to PQC readiness.

Project Planning and Delivery Perspective

IT managed services and strong project planning and delivery capabilities are critical to controlling PQC migration costs. Effective planning establishes clear scope, realistic timelines, and resource alignment, reducing the risk of overruns and costly rework. Managed services with mature delivery frameworks enable structured execution, milestone tracking, and proactive issue resolution, ensuring predictability and cost efficiency throughout the migration process.

High delivery maturity also supports integrated governance, standardised workflows, and transparent reporting, which help organisations manage dependencies and maintain momentum. These practices minimise uncertainty, accelerate migration, and safeguard budgets against unexpected disruptions.

Conversely, poor planning or weak delivery capability often results in delays, dependency conflicts, and emergency fixes. Such inefficiencies inflate labour and vendor costs, extend timelines, and increase operational risk. Inadequate governance introduces hidden expenses and budget volatility, undermining confidence in migration outcomes.

Comprehensive project planning and disciplined delivery within managed services provide a structured, reliable approach to PQC readiness. Investing in these capabilities reduces uncertainty, improves execution quality, and ensures a safer, more economical transition to PQC.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4 How can total migration cost be split into CAPEX vs. OPEX for budgeting?

CAPEX Perspective

a. <u>Investment funding budget</u>

Total PQC migration cost includes CAPEX allocated for initial project setup and foundational investments. CAPEX covers one-time program expenditures required to enable PQC readiness, ensuring alignment with strategic security objectives. These targeted investments accelerate readiness by funding essential capabilities that support long-term resilience. Examples include updating governance frameworks, so procurement and development standards mandate PQC compliance.

Integrating these efforts into broader digital transformation and regulatory strategies helps organisations future-proof critical systems against quantum threats while maintaining compliance and risk management goals. Such investments create a scalable foundation for ongoing PQC adoption without recurring operational overhead, reducing uncertainty and cost volatility.

By prioritising CAPEX for governance, standards, and infrastructure, organisations establish a secure, adaptable environment that supports cryptographic evolution and delivers a more predictable, economical path to PQC readiness.

b. <u>Vendor contract management budget</u>

Total PQC migration costs can allocate CAPEX for vendor contract management by funding upfront investments tied to long-term agreements with technology providers. This includes initial licensing fees, multi-year support contracts, and integration services bundled into vendor offerings. CAPEX allocation ensures procurement and managed services costs are covered upfront, reducing reliance on variable OPEX and improving financial predictability. Strategic vendor negotiations can secure volume discounts and lock in pricing, mitigating future cost escalations and renewal risks.

Conversely, poorly structured contracts or short-term deals often lead to higher renewal rates, unexpected expenses, and budget volatility. Effective CAPEX investment in vendor contracts drives cost stability, strengthens migration efficiency, and supports a scalable foundation for PQC readiness.

OPEX Perspective

c. <u>Tools Licensing</u>

Budgeting for PQC migration requires close attention to operational expenses linked to tool licensing. Begin by assessing the licensing model—subscription or perpetual—and factor in renewal cycles, scalability, and migration timelines. Extended projects can increase recurring costs, while vendor pricing adjustments, such as inflation or tier upgrades, may impact forecasts**.**

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Integration complexity often demands additional tools or connectors, each requiring separate licenses. Training and support, frequently billed as add-ons, should also be included. Likewise, premium features for compliance, security, or advanced analytics can significantly raise costs if overlooked during planning.

Proactive evaluation of these elements helps prevent budget overruns and ensures accurate forecasting. By anticipating licensing dependencies and negotiating favourable terms early, organisations can maintain cost predictability and avoid unexpected financial strain during PQC adoption.

d. Supplier Services T&M

When budgeting for PQC migration, controlling operational expenses under a T&M model is essential for managing overall OPEX. Begin by analysing supplier resource rates and estimating hours based on migration complexity, scope, and duration. Longer timelines directly increase labour costs, making accurate scheduling and dependency management critical to avoid overruns.

Scope changes are a major cost driver in T&M engagements. Even minor adjustments can trigger additional charges, so maintaining strict change control and clear governance is vital. Include vendor overheads such as travel, specialised expertise, and surge capacity for peak phases in your forecasts. These hidden costs often accumulate quickly if not anticipated.

Review contract terms for rate escalations or premium charges for niche skills and ensure transparency in billing practices. Establish milestone-based tracking and proactive reporting to monitor consumption against budget. Without these controls, uncontrolled spend can erode financial predictability and inflate migration costs.

Finally, incorporate contingency planning for unexpected delays or resource shortages. Proactive forecasting, combined with structured governance, helps maintain budget discipline and prevents emergency spending. By managing T&M costs strategically—through accurate estimation, strong oversight, and negotiated safeguards—organisations can achieve cost stability and deliver PQC migration efficiently without compromising timelines or quality.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5 What depreciation schedule should be used for replaced hardware?

When budgeting for PQC migration, aligning the depreciation schedule for replaced hardware with organisational accounting standards and asset lifecycle policies is essential. Most IT infrastructure follows straight-line depreciation over three to five years, providing predictable expense allocation and simplifying financial planning.

Consider the remaining book value of retired assets and any accelerated depreciation required for compliance or tax optimisation. These adjustments can impact financial statements and should be factored into migration planning. Additionally, account for disposal costs, residual value, and potential write-offs for hardware rendered obsolete by cryptographic upgrades.

Integrating depreciation schedules with capital expenditure planning helps avoid sudden financial impacts and supports smoother budget transitions. Accurate forecasting ensures transparency and enables balanced OPEX and CAPEX allocation throughout the migration process. By proactively managing depreciation, organisations maintain financial stability while advancing toward PQC readiness.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

6 What contingency percentage (10–30%) should be applied for unforeseen integration failures?

Setting a contingency of only 10–30% for PQC migration is dangerously inadequate and exposes organisations to severe financial and operational risks. PQC introduces unprecedented complexity across legacy systems, compliance frameworks, and multi-platform environments. Integration failures can trigger cascading impacts—unexpected redesigns, vendor escalations, emergency fixes, and prolonged downtime—all of which carry significant cost implications.

Unlike routine upgrades, PQC migration involves cryptographic dependencies that are volatile and unpredictable. Even minor misalignments in algorithms, hardware security modules, or application interfaces can lead to systemic failures requiring urgent remediation. These scenarios often demand specialised expertise, surge capacity, and accelerated procurement, driving costs far beyond a minimal contingency buffer.

A bare minimum contingency of 30–50% should be considered for standard projects, with higher percentages for large-scale or mission-critical environments. This expanded buffer provides financial resilience, covers emergency resources, and mitigates catastrophic overruns. It also safeguards timelines and operational stability against unforeseen technical challenges inherent in PQC migration.

Underestimating contingency not only jeopardises budget integrity but also risks compliance breaches, reputational damage, and service disruption. By adopting a robust contingency strategy, organisations ensure preparedness for uncertainty, maintain governance, and secure a predictable, controlled path to PQC readiness.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

7 What is the total estimated cost per user, per system, or per terabyte of protected data?

When preparing a PQC migration budget, costs vary widely across cloud, on-premises, and CNI environments. Cloud platforms like AWS and Azure typically offer lower per-user costs—benchmarks could range from $50–$150 per user or $200–$300 per terabyte of protected data, thanks to elasticity and managed cryptographic services. For example, AWS has integrated NIST-approved PQC algorithms into services like KMS and TLS, reducing migration complexity for customers.

In contrast, on-premises deployments, common in financial institutions, incur significantly higher costs—$5,000–$15,000 per system—due to hardware refresh, fragmented cryptographic inventories, and compliance audits under frameworks like PCI DSS 4.0 and DORA. Banks could face additional expenses for vendor-provided PQC solutions and skilled cryptography engineers, which remain scarce.

For CNI sectors such as defence and energy, costs escalate dramatically, exceeding $20,000 per system and $500 per terabyte, driven by zero-downtime requirements, redundancy, and stringent regulatory mandates. U.S. federal agencies, for instance, project $7.1 billion in PQC migration costs by 2035, reflecting the scale and complexity of securing national systems against “harvest-now, decrypt-later” threats.

These metrics underscore the need for risk-adjusted budgeting. Organisations must factor in infrastructure type, compliance obligations, cryptographic agility, and operational resilience. Real-world cases show that underestimating these variables leads to overruns exceeding 30–50%, making robust contingency planning essential for PQC migration success.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

8 How should total PQC migration cost be divided into CAPEX (one-off investments) and OPEX (ongoing operational expenses)?

PQC migration is a multi-year transformation requiring strategic financial planning. Costs should be divided into CAPEX for upfront investments in infrastructure, tooling, and initial implementation, and OPEX for recurring operational activities such as monitoring, maintenance, and vendor support. CAPEX ensures readiness and resilience through foundational upgrades, while OPEX sustains cryptographic agility and compliance over time. Impact factors include regulatory mandates (e.g., NCSC timelines), vendor maturity, asset complexity, and operational scalability. A balanced approach mitigates risks of rushed remediation and uncontrolled consumption, aligning with long-term security and financial agility goals.

CAPEX Perspective

a. <u>Cryptographic Discovery Tooling</u>

Investing in cryptographic discovery tooling is a foundational step in PQC migration. These specialised tools perform comprehensive inventory scans to identify all cryptographic assets across applications, databases, and network endpoints. They also detect vulnerabilities, deprecated algorithms, and weak key lengths, enabling accurate prioritisation of remediation efforts. This one-time investment ensures organisations have complete visibility into their cryptographic landscape, reducing the risk of overlooked dependencies during migration. By automating discovery and reporting, these tools save significant manual effort and accelerate planning. Without this upfront investment, organisations risk fragmented migration strategies, compliance gaps, and costly rework later. Cryptographic discovery tooling is therefore a critical capital expense for building a secure and efficient PQC roadmap.

b. <u>Infrastructure Upgrades</u>

Infrastructure upgrades represent one of the most significant capital investments in PQC migration. Legacy hardware—including servers, network devices, and HSMs—often lacks support for quantum-safe algorithms, making replacement or enhancement unavoidable. Upgrading to PQC-ready infrastructure ensures compatibility with emerging cryptographic standards while future-proofing systems against quantum threats.

Beyond security, these upgrades deliver improved performance, scalability, and operational efficiency, enabling organisations to maintain resilience without compromising speed or reliability. While the upfront cost is substantial, this investment mitigates long-term risks such as system failures, compliance breaches, and emergency remediation expenses.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Modernising infrastructure early creates a stable foundation for PQC adoption, reducing disruption and simplifying integration with evolving cryptographic frameworks. By aligning these upgrades with broader transformation initiatives, organisations can optimise cost, enhance security posture, and ensure seamless migration to quantum-safe environments.

c. Initial Migration & Integration

Initial migration and integration form the cornerstone of PQC readiness, requiring the development and deployment of quantum-safe frameworks across critical systems. This process involves implementing PQC-compliant algorithm libraries, updating application code, and integrating secure key management solutions to ensure cryptographic integrity. These activities demand substantial upfront investment in development resources, robust testing environments, and specialised expertise capable of addressing complex interoperability challenges.

The primary objective is to achieve seamless compatibility between existing systems and new cryptographic standards without compromising functionality, performance, or security. A fragmented approach—where components are upgraded in isolation—can lead to costly future fixes, operational inefficiencies, and compliance gaps. By addressing migration holistically, organisations reduce integration risks and maintain architectural consistency across platforms.

This one-time capital expenditure establishes a secure baseline for cryptographic operations, enabling long-term resilience and adherence to regulatory mandates for quantum-safe security. Beyond compliance, early modernisation minimises disruption during subsequent upgrades and supports scalability for evolving cryptographic frameworks.

Investing in comprehensive migration and integration upfront is not merely a technical necessity—it is a strategic imperative. It ensures predictable outcomes, mitigates operational risk, and positions organisations for sustained security in a PQC era.

OPEX Perspective

a. Continuous Monitoring & Compliance

Continuous monitoring and compliance activities ensure cryptographic systems remain secure and aligned with evolving PQC standards. This involves routine audits, algorithm performance evaluations, and vulnerability assessments to detect weaknesses early. Organisations must also track regulatory updates and implement necessary changes promptly. These recurring tasks require dedicated resources and specialised tools, making them an ongoing operational cost. Without consistent monitoring, risks of non-compliance and exposure to emerging threats increase significantly, jeopardising both security posture and business continuity.

b. Vendor Support & Licensing

Vendor support and licensing costs cover subscription-based services for PQC-enabled platforms, cloud integrations, and managed security solutions. These services deliver essential updates, patches, and technical assistance to maintain cryptographic agility and operational resilience. As PQC standards evolve, vendors release new algorithm libraries and compliance features that organisations must adopt to remain secure and meet regulatory requirements.

Licensing models typically scale with usage, offering flexibility but introducing recurring expenses that must be factored into operational budgets. This investment ensures timely access to expert support, reducing downtime and mitigating risks associated with outdated or unsupported cryptographic implementations. By prioritising vendor support and licensing, organisations safeguard continuity, maintain compliance, and enable a smooth transition to quantum-safe environments.

c. Training & Capability Building

Training and capability building are essential for sustaining organisational readiness during and after PQC migration. These initiatives include periodic workshops, certification programs, and awareness sessions tailored for technical teams and business stakeholders. As cryptographic standards and best practices evolve, employees must remain informed to implement secure solutions effectively and maintain compliance.

Training programs should also address incident response and risk management strategies, equipping teams to handle emerging threats with confidence and agility. By embedding these practices into daily operations, organisations foster a culture of security and accountability, reducing human error and operational vulnerabilities.

Continuous education is often underestimated but represents a critical operational investment. It strengthens resilience, ensures consistent adherence to regulatory requirements, and maximises the return on initial PQC investments. Ultimately, capability building is not a one-time effort—it is an ongoing commitment that safeguards long-term security and operational stability in a rapidly changing cryptographic landscape.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

9 What proportion of total cost should typically be allocated to?

1. Hardware acquisition or replacement?

Hardware acquisition often represents the largest capital investment in PQC migration. Quantum-safe algorithms demand significantly higher computational resources, which many legacy systems cannot support. Organisations should anticipate replacing or upgrading servers, network devices, and HSMs to ensure compatibility with PQC standards and maintain cryptographic integrity.

This category can account for 40–50% of the total migration budget, depending on infrastructure scale and cryptographic workload. Key cost drivers include the lifecycle stage of existing hardware, vendor readiness for PQC compliance, and integration complexity with current systems. Early investment in PQC-ready hardware reduces future remediation costs, minimises operational disruption, and accelerates migration timelines.

Additionally, redundancy and failover systems should be considered to maintain resilience during transition phases. While upfront costs are substantial, these upgrades deliver long-term benefits by enabling cryptographic agility and supporting future algorithm transitions without repeated large-scale replacements. Strategic planning for hardware acquisition ensures a secure, scalable foundation for PQC adoption and positions organisations for sustained security in a PQC era.

2. Software licensing and re-engineering?

Software-related costs can represent a significant portion of PQC migration budgets. Traditionally, cybersecurity projects allocate 30–35% for software, but PQC migrations may push this figure to 60–70% due to extensive cryptographic integration, testing, and licensing requirements. These costs include PQC-compliant libraries, cryptographic frameworks, and re-engineering of applications to support quantum-safe algorithms.

Most existing applications rely on RSA or ECC, requiring substantial code refactoring to integrate algorithms such as Kyber or Dilithium. This process often involves updating APIs, key management systems, and implementing hybrid cryptographic mechanisms to maintain backward compatibility during transition. Licensing costs may include subscriptions for PQC-enabled platforms and cloud services, which provide scalability and vendor support but introduce recurring expenses.

Additional factors influencing cost include application complexity, vendor dependency, and regulatory compliance requirements. Organisations must also budget for interoperability testing to ensure seamless integration across heterogeneous environments, avoiding fragmented implementations that could lead to costly future fixes.

Investing in robust software architecture upfront mitigates these risks, supports operational continuity, and ensures alignment with emerging cryptographic standards. While software-related costs are substantial, they are critical for enabling secure, scalable, and compliant PQC adoption—positioning organisations for long-term resilience for PQC.

3. Testing and certification?

Testing and certification are critical to ensuring PQC implementations meet stringent performance, security, and compliance benchmarks. Organisations should allocate approximately 20% of the total migration budget to this category, as it encompasses multiple essential activities. These include skills retraining for cryptographic functional analysis, security performance baseline testing, and interoperability validation across diverse systems and platforms.

Certification costs often involve third-party audits and adherence to recognised standards such as NIST PQC guidelines or CNSA 2.0. The level of investment depends on regulatory mandates, industry-specific compliance frameworks, and the complexity of cryptographic dependencies within the organisation's architecture. Testing environments must replicate real-world conditions to uncover latency issues, handshake failures, and algorithmic vulnerabilities before production deployment, reducing the risk of operational disruption.

Certification provides assurance to stakeholders, regulators, and customers, mitigating liability and reputational risks associated with non-compliance or cryptographic weaknesses. Despite its importance, testing and certification are frequently underestimated, leading to gaps that can compromise security and increase remediation costs.

Organisations should plan for iterative testing cycles, as PQC migration is not a one-time event but an evolving process requiring continuous validation. By investing in rigorous testing and certification upfront, businesses strengthen cryptographic resilience, maintain compliance, and ensure a secure, predictable transition to quantum-safe environments.

Funded by the European Union

Funded by the European Union under Grant Agreement 101190305. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Disclaimer

This document does not represent the opinion of the European Union or European Commission, and neither the European Union nor the granting authority can be held responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain Q-PREP consortium parties, and may not be reproduced or copied without permission. All Q-PREP consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the Q-PREP consortium as a whole, nor a certain party of the Q-PREP consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk and does not accept any liability for loss or damage suffered by any person using this information.