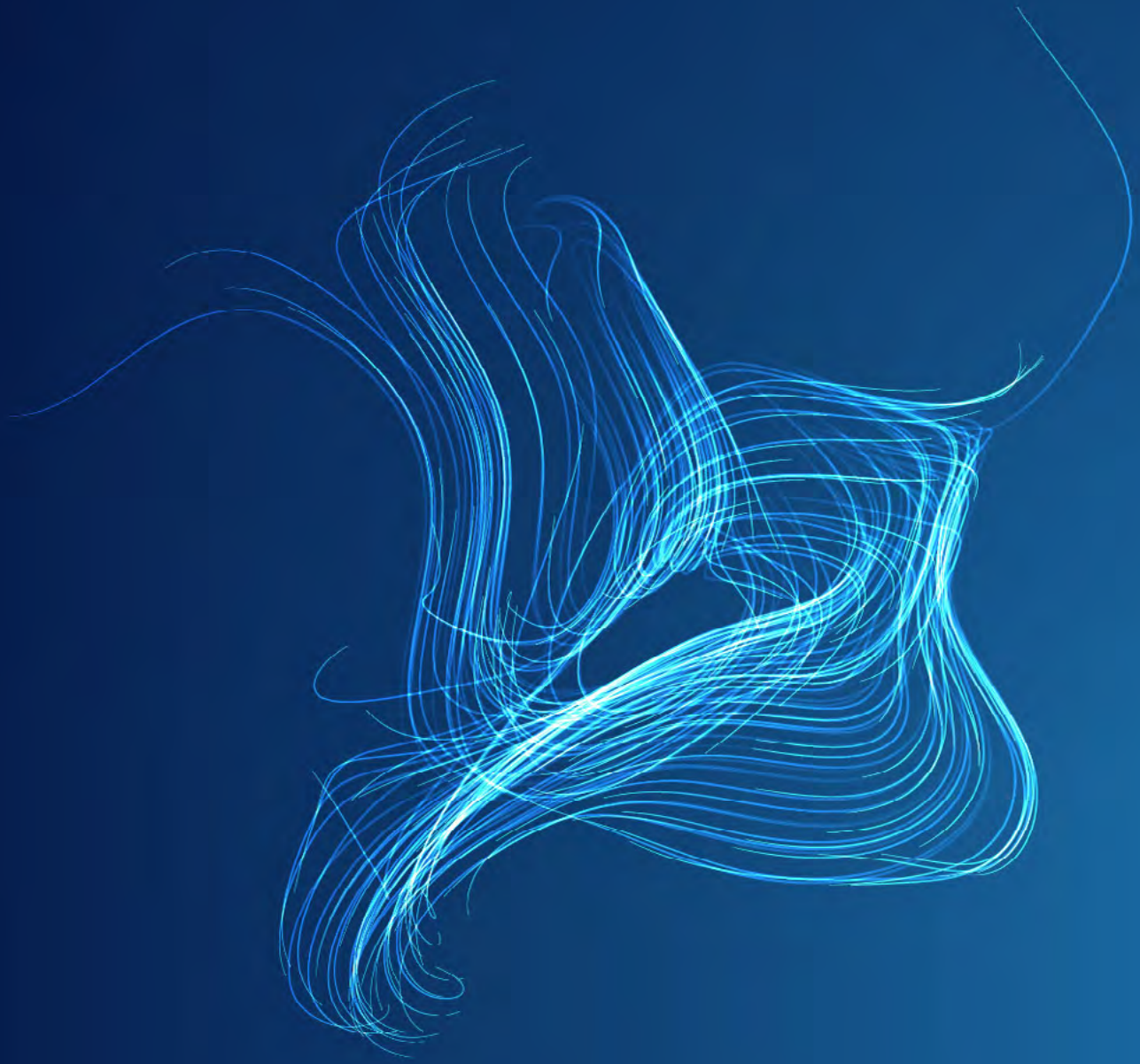
EUROPOL

FS-ISAC

QRWGCFDIR
Quantum-Readiness Working Group of the Canadian Forum for Digital Infrastructure Resilience

QSFF
QUANTUM SAFE FINANCIAL FORUM



PRIORITISING POST-QUANTUM CRYPTOGRAPHY MIGRATION ACTIVITIES IN FINANCIAL SERVICES

PRIORITISING POST-QUANTUM CRYPTOGRAPHY MIGRATION ACTIVITIES IN FINANCIAL SERVICES

PDF Web | ISBN 978-92-9414-091-3 | DOI: 10.2813/9782176 | QL-01-25-027-EN-N

Luxembourg: Publications Office of the European Union, 2026

This publication is a collaborative effort by multiple contributors from various organisations. Their names are included herein.

Cite this publication: Europol, Prioritising post-quantum cryptography migration activities in financial services, Publications Office of the European Union, Luxembourg, 2026.

This publication and more information on Europol are available on the internet.
www.europol.europa.eu

CONTENTS

EXECUTIVE SUMMARY

As post-quantum cryptography (PQC) becomes integrated into mainstream information technology (IT) products and services, financial services institutions must begin to execute their transition strategies. This document provides actionable guidelines to incorporate quantum safety into existing risk management frameworks by assessing the **'Migration Priority'** based on the **'Quantum Risk'** and **'Migration Time'** of business use cases and highlighting opportunities for immediate execution.

A critical first step is to **inventory all business use cases that rely on public key cryptography**. This inventory enables the creation of a prioritised transition roadmap by assessing the **Quantum Risk** of each use case based on three parameters:

- **Shelf Life of Protected Data:** How long the data remains sensitive.
- **Exposure:** The extent to which data is accessible to potential attackers.
- **Severity:** The business impact of a potential compromise.

When the **Quantum Risk** is assessed, organisations can prioritise actions based on each use case's **Migration Time**, i.e., the complexity and timeline required to achieve Quantum Safety for a use case. As part of this activity, organisations will identify, for instance, actions that can be launched immediately and the use cases that require coordination with long-term asset lifecycles.

- **Solution Availability:** Maturity of PQC standards, and their general availability in products and services.
- **Execution Cost:** The effort, cost, and complexity of implementing the quantum-safe solutions within the organisation.
- **External Dependencies:** Execution complexity due to coordination required with third parties and their transition roadmaps (standardisation bodies, vendors, peers, regulators, and customers).

Examples of use cases that financial organisations can begin implementing today include:

- Integration of **post-quantum requirements** into the long-term roadmap for hardware-intensive use cases aligned with financial asset lifecycles.
- Enhancement of **confidentiality protection for transactional websites.**
- Identification and elimination of **cryptographic antipatterns** to reduce future technical debt.

These are examples of how financial institutions can take timely, structured steps toward an efficient and forward-looking transition to post-quantum cryptography.

CONTRIBUTORS

Oscar Covers, Dutch Banking Associations (NVB)

Dr. Thibaud Ecarot, National Bank of Canada

Rebecca Gibergues, FS-ISAC

Jaime Gómez García, Banco Santander

Francis Gorman, Bank of Ireland

Imran Khan, BMO

Ivan Makarov, TD Bank

Sarah McCarthy, Citi

Michele Mosca, University of Waterloo

Iván Soto, Banco de España

Leila Taghizadeh, Allianz

Jelena Zelenovic, EIB

ENDORSEMENTS

Allianz

Banco Santander

Bank of Ireland

CertFin Italy

Dutch Banking Association (NVB)

Euroclear

European Investment Bank (EIB)

KBC Belgium

LGT

Mizuho

PostFinance

DISCLAIMER

This document is produced by subject matter experts from participating financial institutions. It is intended for professional development, knowledge-sharing, and community outreach purposes. The content reflects the collective insights of contributors and does not constitute legal, regulatory, or policy advice.

This document is not mandatory for implementation or endorsement by any participating organisation, nor does it impose or infer any obligations on its contributors, endorsers, or their institutions, who remain free to determine their own policies and strategies in relation to the topics discussed. There are no intellectual property claims or liabilities associated with its use. Organisations may reference or adapt the content at their discretion without any responsibility attributed to the cyber experts or their institutions.

The contributors do not guarantee the accuracy, completeness, or suitability of this document for any specific purpose. It should not be relied upon as formal guidance for regulatory compliance or supervisory engagement.

QUANTUM-SAFETY PRIORITISATION

As post-quantum cryptography integrates into mainstream IT products and services, financial organisations must transition from strategy design to execution. A critical first step is to create and maintain an inventory of all business use cases that rely on public key cryptography. This paper provides a simple methodology organisations can use to assess the **Migration Priority** of each use case as a function of **Quantum Risk** and **Migration Time**. This ensures that mitigation efforts focus where the impact is most significant and provides actionable guidelines to incorporate Quantum Safety into existing risk management frameworks.

By evaluating the **Migration Priority** of their use cases, organisations can gain valuable insights to guide strategic decision-making, helping them answer critical questions such as:

- **Is urgent action important?** Clarifying the potential business, operational, and reputational impacts of inaction.
- **What is the cost–benefit of acting sooner rather than later?** Evaluating the trade-offs between early adoption and delayed migration, particularly in light of evolving market opportunities and technology readiness.
- **When should we act?** Understanding the priorities based on **Quantum Risk** exposure and implementation complexity to determine the optimal timing for initiating migration activities.
- **What are our dependencies?** Identifying internal or external supply chain factors that could influence execution timelines.
- **Do we have the required capacity?** Evaluating whether internal expertise and execution capabilities are adequate for our organisation's change roadmap, or if additional support is needed.
- **Is our plan effective?** Assessing whether available and planned resources, technologies, and coordination efforts support a timely and successful transition.

Assessing Risk with a Quantum Risk Score

The **Quantum Risk Score** quantifies the risk of not achieving quantum safety and captures the urgency of transitioning a given use case. The **Quantum Risk Score** is based on three parameters:

- **Shelf Life of Protected Data** (X in Mosca's Theorem[1]): How long the data remains sensitive.
- **Exposure:** The extent to which data is accessible to potential attackers.
- **Severity:** The business impact of a potential compromise.

These parameters are rated on a 1–3 scale, where level 1 represents the lowest or least severe risk, level 2 represents a moderate or intermediate risk, and level 3 represents the highest or most severe risk.

FACTOR	SCALE (1–3)
SHELF LIFE	1 = <2 years (short-term) 2 = 2–5 years (medium-term) 3 = >5 years (long-term)
EXPOSURE	1 = Data accessed over owned infrastructure only 2 = Data access is limited to specific third parties 3 = Data is publicly accessible or can be easily leaked
SEVERITY	1 = Minimal impact (reputational at most) 2 = Relevant business impact 3 = Severe disruption

The score is calculated as:

Quantum Risk Score = round (sum of factors ÷ 3)

A higher score indicates higher **Quantum Risk**.

1 https://en.wikipedia.org/wiki/Michele_Mosca#Mosca's_theorem

Assessing Migration Time

The **Migration Time Score** (Y in Mosca's Theorem) reflects the complexity and timeline required to achieve Quantum Safety for a use case. It is determined by:

- **Solution Availability**: Maturity of PQC standards, and their general availability in products and services.
- **Execution Cost and Time**: The effort, cost, and complexity of implementing the quantum-safe solutions within the organisation.
- **External Dependencies**: Execution complexity due to coordination required with third parties and their transition roadmaps (standardisation bodies, vendors, peers, regulators, and customers).

Rated on a 1–3 scale:

FACTOR	SCALE (1–3)
SOLUTION AVAILABILITY	1 = Available now or <1 year 2 = Expected in 1–3 years 3 = Uncertain or >3 years
EXECUTION COST AND TIME	1 = Minor reconfigurations as part of business as usual (BAU) 2 = Moderate architectural changes 3 = Major, uncertain, or costly upgrades (e.g., logistically complex hardware replacements)
EXTERNAL DEPENDENCIES	1 = Minimal or already widely adopted 2 = Dependent on third parties with known 1 to 3-year roadmaps 3 = Dependent on third parties with uncertain or > 3-year roadmaps

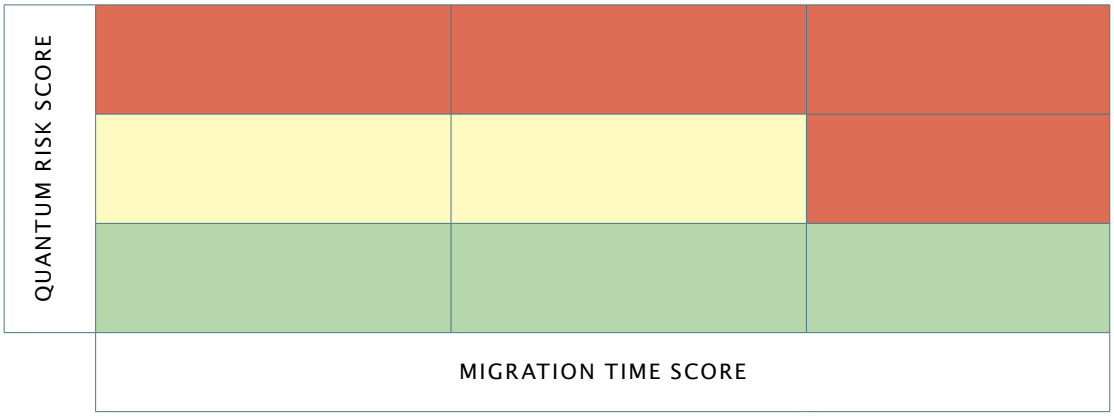
The score is calculated as:

Migration Time Score = round (sum of factors ÷ 3)

A higher score indicates greater execution complexity.

Determining Migration Priority

By combining **Quantum Risk Score** and **Migration Time Score**, organisations can classify use cases into **High**, **Medium**, or **Low** priority according to a risk–time matrix:



High Priority (Red)

1. **High-risk use cases with readily available solutions**: 'Low-hanging fruit' for immediate transition.
2. **High-risk use cases requiring preparation**: Should be included in the roadmap with near-term planning (budget allocation, platform upgrades, prerequisites). No-regret technical activities should be initiated as pre-work for the transition.
3. **High and medium-risk use cases with long dependencies**: Require long-term planning, assessing the critical factors and actions required to ensure timely completion.

Medium Priority (Yellow)

4. **Medium-risk use cases with short migration paths**: May be included in BAU upgrades.
5. **Medium-risk use cases requiring planning**: Should be tracked to determine optimal preparation timelines. No-regret technical activities may be initiated as pre-work for the transition.

Low Priority (Green)

6. **Low-risk use cases**: Can be addressed opportunistically through standard modernisation programmes.

This framework provides a structured, business-oriented approach for prioritising the quantum-safe transition. By assessing both risk exposure and migration complexity, organisations can align resources with the most urgent and impactful use cases, ensuring resilience against the quantum threat.

The most valuable outcome of the prioritisation exercise, however, is not the individual scores themselves, but the insights gained through the process, which empower informed, strategic decision-making. **Organisations are encouraged to adapt the framework to their specific context and use the resulting information to guide tailored, evidence-based migration decisions**.

EXAMPLE USE CASES

The following use cases serve as a demonstration of this methodology.

Use case 1: Points of Sale

Points of Sale (PoS) are network endpoint devices where payment transactions are started. PoS directly handle sensitive data such as payment card details, personal identifiers, or loyalty account information. At the same time, they are widely spread and readily available to third parties.

The typical process of a financial transaction conducted through a **Point-of-Sale** system is as follows:

1. **Transaction initiation:** The customer presents their payment card to the PoS terminal to initiate the transaction.
2. **Data capture and transmission:** The PoS captures the payment details. In *online mode*, these details are transmitted to the merchant's bank for authorisation using symmetric key cryptography. In *offline mode*, the payment data is verified with public key signatures and stored for later transmission, with authorisation decisions made locally based on predefined rules.
3. **Routing through the payment network:** The merchant's bank forwards the payment request, via the appropriate payment scheme, to the customer's issuing bank.
4. **Authorization:** The issuing bank verifies the payment details and sends back an authorization response.
5. **Completion:** The authorisation message travels back through the same route to the PoS terminal, which displays the result and completes the transaction, either approving or declining it.

Throughout this process, the transaction flow is protected by multiple cryptographic mechanisms, combining symmetric and public key cryptography to ensure confidentiality, integrity, and authenticity.

A detailed analysis of the cryptography involved and quantum-safety considerations can be found in EMVCo's "Quantum Computing and EMV® Chip – What's the Threat?"[2] and FS-ISAC's 'Post Quantum PCI Use Cases: ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems'[3].

2 https://www.emvco.com/knowledge-hub/quantum-computing-and-emv-chip-whats-the-threat/
3 https://www.fsisac.com/pqc-payment-card-industry

According to EMVCo's analysis, the most relevant quantum threat to the payment cards ecosystem is breaking a Payment System or Issuer's public key, as it would allow the production of fake cards used for fraudulent offline payments.

Prioritisation analysis

Quantum Risk

The **Quantum Risk** associated with compromising the authentication of offline card transactions by calculating the Payment System or Issuer's private key can be assessed as follows:

FACTOR	SCALE (1-3)	DESCRIPTION
SHELF LIFE	3	The issuer's public key is used to generate cards that are expected to be **valid over several years**.
EXPOSURE	3	Both payment cards and PoS terminals are **publicly accessible**, increasing the likelihood of data exposure to potential attackers.
SEVERITY	1	According to EMVCo, the impact would be limited to the production of fake cards used for fraudulent offline payments. While this would disrupt a part of the payment cards ecosystem, it would not have an impact on the largely predominant use case of online payments, and some offline payments could be forced to be online as a mitigation. However, use cases that rely on offline payments to support limited connectivity, reduce latency, or ensure resilience during outages would remain vulnerable to fraud.

Quantum Risk Score: 2 Medium

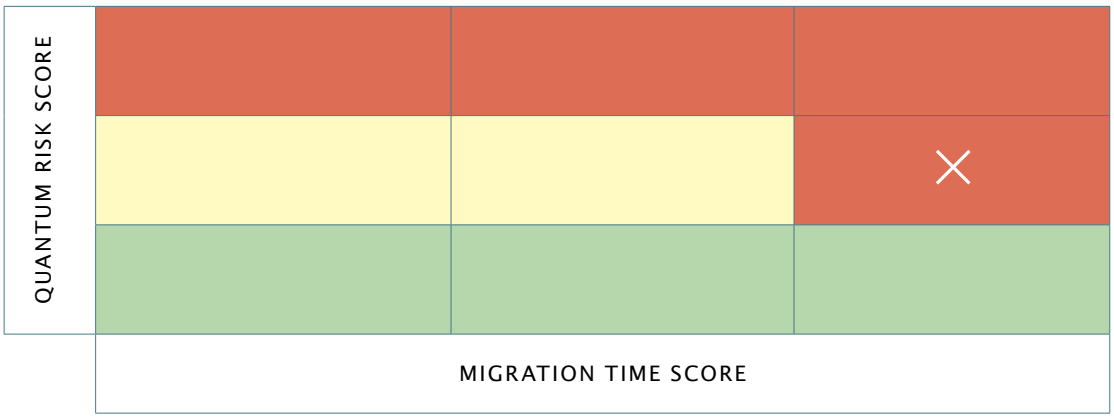
Migration Time

The **Migration Time** associated with compromising the authentication of offline card transactions by calculating the Payment System or Issuer's private key can be assessed as follows:

FACTOR	SCALE (1–3)	DESCRIPTION
SOLUTION AVAILABILITY	3	EMVCo has indicated its intention to identify cost-effective security solutions whose implementation timeline is commensurate with the quantum threat being realised. As of the publication of this report, EMVCo has not announced plans to integrate PQC into its specifications nor provided a roadmap for taking it into account.
EXECUTION COST AND TIME	3	PoS terminals are typically owned or leased by merchants. Given the uncertainty surrounding final PQC implementations, any required hardware upgrades could have a significant cost and logistical impact due to the vast number of terminals in circulation. With typical upgrade cycles spanning 5–7 years, premature replacement would disrupt established depreciation lifecycles and introduce substantial additional costs.
EXTERNAL DEPENDENCIES	3	The PoS ecosystem involves multiple stakeholders and overlapping responsibilities, including PCI, Europay, Mastercard, and Visa (EMV), Common Payment Application Contactless Extension (CPACE), payment service providers (PSPs), and smartcard and terminal manufacturers. Achieving a coordinated transition will require complex orchestration and alignment across these entities.

Migration Time Score: 3 High

Migration Priority



Medium-risk use cases with long dependencies: require long-term planning, assessing the critical factors and actions required to ensure timely completion.

The migration to quantum-safe cryptography within the PoS ecosystem presents high implementation complexity due to the diverse stakeholder landscape, hardware dependencies, and evolving standardisation efforts. The **Migration Priority Score** of PoS terminals is therefore assessed as **High**, reflecting the intricate interplay within the payments ecosystem and the potential costs associated with out-of-cycle hardware replacements.

Early consideration of hardware requirements to support PQC will deliver direct cost reduction benefits, as it would help avoid premature replacements before the planned end-of-life (EOL) of existing terminals. Although standardisation is progressing, the lack of concrete implementation timelines and the logistical scale of deployment make this a long-term, resource-intensive transition. Consequently, PoS systems should be included in early planning phases to ensure readiness once post-quantum standards and certified hardware solutions become available.

Some recommended immediate actions include:

- **Assess the relevance of offline** payments within your business, including their use as a resiliency measure, and the potential impact of a signing key compromise.
- **Map the end-to-end supply chain** to identify dependencies, monitor ecosystem developments, and understand the transition roadmaps of key stakeholders.
- **Collaborate across the industry** to establish a coordinated and consistent transition timeline, aligning efforts among financial institutions, vendors, and standards bodies.
- **Evaluate mitigations** such as enforcing online verification or implementing detective controls.
- **Inventory all public key infrastructure (PKI) components** involved in card payment processes to assess cryptographic exposure and prioritise migration planning.

Use case 2: Public websites

Banks and other financial institutions rely extensively on public-facing websites to interact with customers and provide online services. These digital channels involve multiple layers of authentication and encryption, each playing a vital role in protecting sensitive information.

At the infrastructure level, Transport Layer Security (TLS) authentication is performed interactively for each session based on public key certificates. These certificates are currently vulnerable to quantum attacks due to their reliance on classical public key cryptography.

At the user level, authentication mechanisms vary. Traditional password-based authentication requires measures to protect credential confidentiality, while passwordless approaches such as Fast Identity Online (FIDO), use public key cryptography, where the user's device signs a challenge with a private key and the server verifies it using the corresponding public key. These methods are considered secure today; however, they would become vulnerable if an attacker were able to derive private keys before their expiry using quantum computing capabilities.

Website communications frequently transmit confidential data, including customer credentials, personal details, and financial information. Such data may be subject to retention requirements of several years (for example, seven years in certain jurisdictions). Even after the retention period has expired, the unauthorised disclosure of historical data could still result in significant reputational damage.

Confidentiality protection for these communications is provided through TLS session encryption. To achieve quantum-resistant security, TLS implementations will need to adopt quantum-safe encryption algorithms and post-quantum key agreement schemes.

This represents the most immediate quantum threat for public websites: the risk of 'harvest-now, decrypt-later' attacks, where adversaries collect encrypted traffic today with the intention of decrypting it once quantum capabilities become available.

Prioritisation analysis

Quantum Risk

The **Quantum Risk** associated with compromising the confidentiality of a website handling customers' private financial data can be assessed as follows:

FACTOR	SCALE (1-3)	DESCRIPTION
SHELF LIFE	3	Customer financial and personal data must be protected over the long term, as its sensitivity and regulatory retention requirements often extend for several years.
EXPOSURE	2	The data is transmitted over public networks between the website and user devices. While interception is technically possible, it would typically require large-scale monitoring and long-term storage, limiting feasibility to highly motivated and targeted adversaries.
SEVERITY	2	A systemic loss of confidentiality in transmitted data would result in significant reputational and compliance impacts. However, leakage of historical data, while relevant, would likely not be sufficient to cause sustained business disruption.

Quantum Risk Score: 2 Medium

Migration Time

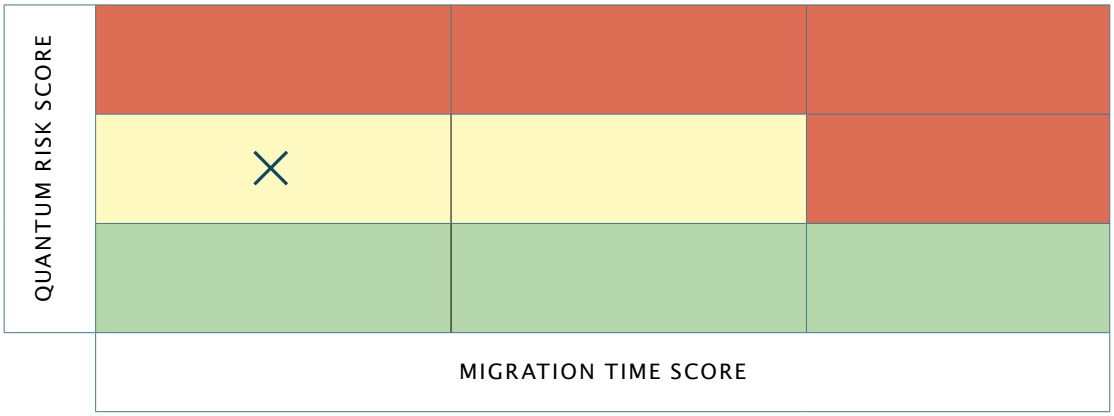
The **Migration Time** associated with compromising the confidentiality of a website handling customers' private financial data can be assessed as follows:

FACTOR	SCALE (1–3)	DESCRIPTION
SOLUTION AVAILABILITY	1	The hybrid post-quantum/classical key agreement scheme X25519MLKEM768 is already configured as the default in the latest versions of most major cryptographic libraries. Leading server operating system vendors have announced or released support for these versions, with widespread availability expected before the end of 2026. Furthermore, the largest content delivery network (CDN) providers, which are commonly used to deliver public website content, already support or have short-term roadmaps to support X25519MLKEM768.
EXECUTION COST AND TIME	1	Deployment across the client–CDN connection is expected to be seamless, as the configuration will either be enabled by default or require only minimal adjustments. On the server–CDN side, implementation will involve standard software upgrades and minor reconfigurations, resulting in negligible operational disruption.
EXTERNAL DEPENDENCIES	1	Most web browsers have supported X25519MLKEM768 since November 2024, and this quantum-safe configuration has already undergone extensive field testing. It is currently supported by five of the world's top 10 websites, demonstrating market maturity and interoperability.[4]

Migration Time Score: 1 Low

4 https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web

Migration Priority



Medium-risk use cases with short migration paths: may be included in BAU upgrades.

The primary quantum threat vector for public websites stems from harvest-now, decrypt-later attacks, in which adversaries capture encrypted traffic today with the intent to decrypt it once quantum computing capabilities become available.

Fortunately, hybrid post-quantum TLS mechanisms, such as X25519MLKEM768, are already supported across major web browsers, cryptographic libraries, CDNs, and operating systems. Although this key agreement scheme has not yet completed its formal standardisation process, its widespread adoption and field testing over several months have effectively established it as a de facto industry standard.

Public websites present a medium **Quantum Risk** but a low **Migration Time**, making them strong candidates for early adoption of quantum-safe cryptography. Although the confidentiality of transmitted customer data remains long-lived, the technical and operational effort required for migration is minimal.

Despite being rated as a **Medium** risk in overall migration priority, this use case provides the earliest practical opportunity for financial institutions to deploy post-quantum protections in production environments, largely enabled by CDN providers. Financial institutions should monitor the adoption of X25519MLKEM768 across their supply chain and take advantage of this readiness to implement quantum-safe TLS configurations quickly and cost-effectively, safeguarding long-term data confidentiality and reinforcing customer trust in digital services.

Moreover, implementing these early quantum-safe measures offers a valuable opportunity to raise awareness across the organisation among technical teams, decision-makers, and customers about the importance and feasibility of preparing now for a quantum-resilient future.

Some recommended immediate actions include:

- **Verifying the PQC readiness roadmap** of all platforms involved in exposing in-scope websites to the Internet, such as web servers, reverse proxies, web application firewalls (WAFs), and CDNs.
- **Piloting the deployment** of the X25519MLKEM768 hybrid key agreement scheme on representative but non-critical websites to evaluate interoperability and performance impacts.
- **Implementing X25519MLKEM768 support** as appropriate, following the remediation of all issues identified during the testing phase.

CRYPTOGRAPHIC ANTIPATTERNS

In cybersecurity, an antipattern is a commonly used yet flawed solution to a recurring problem. It may appear practical or convenient at first, but ultimately introduces vulnerabilities, increases risk, and makes systems harder to secure and maintain over time, resulting in unwanted technical debt.

In the financial sector, which handles highly sensitive information such as personal data, authentication credentials, and transaction details, cryptographic antipatterns can expose institutions to data breaches, fraud, regulatory non-compliance, and reputational damage. Moreover, these poor practices can complicate future cryptographic transitions, preventing the adoption of crypto-agile methodologies that are essential for responding to emerging threats.

Given the complex IT environments of large financial organisations and the continued presence of legacy systems and products, identifying and remediating cryptographic antipatterns early in the quantum-safety migration process offers multiple benefits. It allows institutions to:

- Strengthen cryptographic configurations and governance.
- Reduce immediate operational and security risks.
- Increase cryptographic maturity and agility.
- Accelerate migration through no-regret actions, even for use cases not yet ready for full execution.

Antipattern sets can be defined for different use cases, identifying specific remediation activities and their corresponding no-regret benefits. For example, organisations can identify undesirable coding practices within software repositories:

ANTIPATTERN	REMEDIATION	NO-REGRET BENEFIT
Hard-coded credentials, defaults, and cryptographic configuration parameters.	Implement automatic discovery of hard-coded credentials and cryptographic key materials in the code before deployment. Apply the same validation retroactively to existing code. Migrate key materials to protected storage. Use secure key management systems. Move configuration parameters to configuration files and environment variables.	Improved security & regulatory compliance posture, reduced operational risk, raised cryptographic maturity, and crypto agility.

While some remediations may be challenging to implement, organisations can prioritize them based on value versus implementation cost, similar to the use case prioritisation framework, but replacing the **Quantum Risk** dimension with a **Benefit** assessment.

As part of the prioritisation exercise, public websites were identified as an ideal candidate for early modernisation toward quantum-safe cryptography. The following table describes five common cryptographic antipatterns affecting public websites and suggests some recommended remediations:

ANTIPATTERN	REMEDIATION	NO-REGRET BENEFIT
Manual management of TLS certificates.	Implement automated certificate management for deployment, renewal, rotation, and revocation.	Minimises future migration complexity and execution cost, reduces operational risk, and enhances crypto agility.
Heterogeneous TLS configurations.	Establish a standardised TLS configuration baseline across all environments. Implement mechanisms to automate TLS configuration management for consistency and auditability. Target full adoption of TLSv1.3 (a prerequisite for post-quantum cryptography) and strong cryptographic algorithms.	Simplifies configuration control and compliance management. Enables crypto-agile configuration practices, minimising future remediation efforts. Accelerates alignment with PQC readiness requirements.
Maintaining outdated backward compatibility (e.g., TLSv1.0/1.1 or weak ciphers).	Implement controls to monitor **TLS handshakes** and track negotiated versions, cipher suites, and key agreement schemes. Use this data to assess and phase out legacy dependencies.	Identifies legacy dependencies and supports long-term compliance. Prepares the control framework for future decommission of vulnerable configurations.
Pinning to uncontrolled certificates	Adopt modern certificate management and monitoring practices, including Certificate Transparency logs and CAA records, to prevent mis-issuance.	Reduces outage risk, improves crypto agility, and prepares for shorter certificate lifespans in future standards.
Use of wildcard host certificates	Replace with hostname-specific certificates.	Reduces the risk of large-scale compromise and limits potential misuse of certificates.

Identifying cryptographic antipatterns and understanding their impact is a multidisciplinary task requiring collaboration across multiple internal teams. To ensure a structured and effective approach, cryptography leaders should:

- **Collaborate** with Enterprise and Solution Architects, as well as Operations teams, to catalogue known antipatterns based on experience and risk insights.
- **Update** internal security policies and development guidelines to formally include identified antipatterns and ensure all stakeholders recognize them as prohibited practices.
- **Establish metrics and key performance indicators (KPIs)** to monitor remediation progress, linking them to expected benefits to validate the achievement of tangible risk reduction and maturity improvement.

Avoiding cryptographic antipatterns is a foundational step towards building resilient, trustworthy, and crypto agile systems. In the financial industry, where the stakes are exceptionally high, proactively remediating these issues strengthens the institution's security posture, ensures regulatory alignment, and enhances customer trust through actions that can be initiated immediately.

CONCLUSION

The transition to quantum-safe cryptography is not merely a technical upgrade. It is a strategic imperative that demands foresight, coordination, and disciplined execution across the entire ecosystem.

A prioritisation framework enables organisations to make data-driven migration decisions, focusing efforts where risk is highest and change is most feasible. More importantly, the process itself builds a deeper understanding of exposure, dependencies, and readiness, empowering leaders to act with confidence. Each institution should adapt the framework to its own context and translate insights into targeted, achievable actions.

At the same time, addressing cryptographic antipatterns offers a practical and immediate way to improve overall resilience. These no-regret actions, such as automating certificate management, standardising TLS configurations, and eliminating insecure coding practices, enhance crypto agility, reduce operational risk, and accelerate readiness for post-quantum standards.

The path towards Quantum Safety will be iterative and collaborative, requiring alignment across internal teams, vendors, regulators, and standards bodies. Institutions that begin this journey now by improving visibility, modernising cryptographic practices, and integrating quantum-safe solutions when and where possible will not only safeguard their data and customers, but will also position themselves as leaders in secure digital innovation for the quantum era.