electronics

Article

Towards a Unified Quantum Risk Assessment

Šarūnas Grigaliūnas * and Rasa Brūzgienė

Department of Computer Sciences, Kaunas University of Technology, Studentu Str. 50, 51368 Kaunas, Lithuania; rasa.bruzgiene@ktu.lt
* Correspondence: sarunas.grigaliunas@ktu.lt

Abstract

Quantum computing poses an unprecedented threat to classical cryptography, requiring new risk assessment paradigms. This paper proposes a Quantum-Adjusted Risk Score (QARS) model, a theoretical and methodological innovation within the EU's PAREK framework (Post-quantum asset and algorithm inventory, risk assessment, road mapping, execution, key governance). QARS extends Mosca's inequality—which defines a quantum threat timeline threshold—into a multi-factor risk scoring formula. We formalise QARS with mathematical expressions incorporating timeline, sensitivity, and exposure dimensions, each calibrated by factor weights and scaling functions. The design motivations for including these dimensions are discussed in depth. We present method for model calibration (including sector-specific weight adjustments) and outline validation strategies combining quantitative analysis and expert judgement. The proposed QARS model is situated in the context of the EU's coordinated roadmap for post-quantum cryptography and cybersecurity regulations, illustrating how QARS supports compliance and strategic migration prioritisation. A prototype tool implementing QARS model is also provided to demonstrate practical applicability. Our contributions provide a unified approach to quantum risk assessment, marrying theoretical rigour with policy-relevant risk management needs to help organizations proactively address the quantum threat.

Keywords: quantum risk assessment; post-quantum cryptography; Mosca's inequality; quantum-adjusted risk score (QARS); crypto-agility; PAREK framework; timeline risk; exposure risk; data sensitivity; EU's coordinated PQC roadmap

Academic Editor: Aryya Gangopadhyay

Received: 23 July 2025
Revised: 13 August 2025
Accepted: 21 August 2025
Published: 22 August 2025

Citation: Grigaliūnas, Š.; Brūzgienė, R. Towards a Unified Quantum Risk Assessment. *Electronics* **2025**, *14*, 3338. https://doi.org/10.3390/electronics14173338

1. Introduction

Quantum computers—once regarded as a remote theoretical possibility—are rapidly emerging as a tangible threat to contemporary public-key cryptography. Breakthroughs in quantum algorithm engineering and error correction have compressed the expected "quantum threat timeline." Given the 2030 deadlines in the EU PQC roadmap [1] and increasing regulatory pressure globally, a quantitative risk scoring framework is urgently needed to support rational resource allocation for cryptographic migration. Notably, Gidney and collaborators [2] demonstrated a 20-fold reduction in the logical qubit requirements needed to factor RSA-2048 compared with 2019 estimates, implying that cryptographically relevant quantum computers may arrive far sooner than previously projected.

Conventional cyber-risk analyses often model the quantum threat as a binary future event—so-called "Q-day." This simplification is misleading, because quantum risk is time-coupled: it depends on when an adversary's quantum capability materialises relative to the security lifetime of vulnerable systems and data. Mosca formalised this temporal aspect through the well-known inequality [3]:

$$X + Y > Z, \tag{1}$$

where X is the number of years the data must remain confidential, Y is the years required to migrate to post-quantum cryptography (PQC), and Z is the anticipated time until an adversary acquires a cryptographically relevant quantum computer (CRQC). If Equation (1) holds, confidentiality cannot be assured. Mosca's inequality elegantly highlights the window of vulnerability created by long-lived data and delayed migration, yet it remains coarse-grained, offering a binary threshold without considering other critical factors such as data sensitivity or adversarial exposure.

Despite several proposed emerging frameworks, there remains a lack of a unified, mathematically grounded risk scoring model that can incorporate time-to-break, data sensitivity, and exposure risk in a way that aligns with regulatory demands and operational needs. Mosca's own quantum risk assessment (QRA) process adapts the NIST cyber-risk lifecycle to quantum threats, focusing primarily on the temporal dimension [4]. The Crypto-Agility Risk Assessment Framework (CARAF) advances this by multiplying a timeline factor with an impact–cost factor to emphasise organisational agility [5]. While these approaches underscore timeline urgency and migration readiness, none provides a unified numerical score that integrates when, what and how quantum threats influence each asset. To address this gap, we introduce the Quantum-Adjusted Risk Score (QARS)—the first unified, multi-dimensional model that transforms Mosca's timeline inequality into a continuous, weighted risk score incorporating sensitivity and exposure. This enables precise prioritisation of post-quantum migration across sectors, something not possible with previous binary or checklist-based frameworks.

QARS forms the analytic kernel of the EU-aligned PAREK lifecycle that includes post-quantum asset and algorithm inventory, risk assessment, road mapping, execution, and key governance. Within PAREK, QARS ranks assets according to quantum vulnerability by extending Mosca's timeline concept into a composite score comprising Equation (1):

- A timeline dimension comparing the CRQC horizon to mitigation and confidentiality requirements;
- A sensitivity dimension reflecting the criticality of the protected data or service; and
- An exposure dimension capturing the adversary's practical ability to harvest or intercept quantum-breakable ciphertext.

Adjustable weights allow organizations to calibrate QARS to sector-specific risk appetites, producing a single 0–100 (or 0–1) index that expresses urgency and severity.

The objectives of this work are as follows:

1. To give a formal definition of QARS, including an extended Mosca-based timeline function, factor weightings, and scaling mappings;
2. To justify each dimension theoretically and show how they remedy limitations of prior models;
3. To describe calibration method and validation strategies, including quantitative approach such as scenario analysis and qualitative approach such as expert reviews that align QARS with organisational risk governance;
4. To position QARS within current EU initiatives, notably the Coordinated Implementation Roadmap for PQC [6], and regulatory instruments such as NIS2 [7] and the upcoming Cyber Resilience Act [8].

We additionally reference a proof-of-concept implementation of QARS developed using Streamlit, which illustrates its practical applicability in real-time risk scoring.

However, the specifics of the user interface are considered beyond the scope of this theoretical exposition.

The remainder of the paper is organised as follows: Section 2 provides a survey of existing quantum risk assessment frameworks. Section 3 derives the QARS model and states its underlying assumptions. Section 4 applies QARS to illustrative asset classes and aligns resulting scores with EU risk categories. Section 5 contrasts QARS with existing frameworks, discusses integration with policy and enterprise risk management, and outlines limitations and future work. Section 6 concludes by summarising QARS's significance for advancing quantum-ready cybersecurity.

2. State of the Art in Quantum Risk Assessment

Quantum risk assessment has emerged as a multidisciplinary field, incorporating cryptographic theory, risk modelling, and regulatory alignment. Central to this domain is the forecasting of quantum computing timelines. The Global Risk Institute's 2023 Quantum Threat Timeline report [4] synthesises expert predictions on the emergence of cryptographically relevant quantum computers, emphasising the shrinking window for proactive migration. Kumar in [9] further develops this by introducing timeline-based risk metrics, formalising the notion of vulnerability based on the relation between data shelf-life, migration speed, and quantum adversary capabilities. These studies underscore that risk is not binary (i.e., Q-day), but rather a continuous function of technological, strategic, and operational readiness.

Recent years have seen a surge in comprehensive quantum risk assessment frameworks. Notably, the FS-ISAC Post-Quantum Cryptography Risk Model [10] presents a sector-aligned structure that assesses cryptographic inventory and migration criticality across organisational assets. Similarly, Baseri et al. in their work [11] propose a structured evaluation model incorporating a STRIDE-like decomposition of vulnerabilities in quantum transition contexts. These frameworks advance beyond classical binary assessments and integrate multiple risk facets, including sensitivity, exposure, and cryptographic agility. Meanwhile, Weinberg in [12] introduces QUASAR (Quantum Ready Architecture for Security and Risk Management), a strategic framework mapping operational risk processes to quantum-readiness levels. These models reflect a maturing consensus around the need for multi-factor, asset-specific quantum risk quantification.

In this context, Yang et al. [13] introduced a quantum risk model applied to public health emergencies, using probabilistic simulation and early warning indices. While innovative in adapting quantum concepts to non-cyber domains, the model is highly domain-specific and does not generalise to cryptographic infrastructure. Furthermore, it lacks modular components to integrate exposure and cryptographic shelf-life factors. This model is problem-specific and lacks the scoring generalisability across digital assets.

Woerner and Egger in their work [14] proposed Quantum Risk Analysis (QRA) using quantum algorithms such as amplitude estimation to compute risk metrics like VaR and CVaR. While groundbreaking in leveraging quantum computing for financial risk modelling, their work is focused on the use of quantum algorithms rather than assessing the risks posed by quantum threats to classical systems. Thus, it operates at a different layer than QARS, which is aimed at operational cyber risk quantification in a pre-quantum era.

Ahmad et al. incorporated fuzzy logic and the Analytic Hierarchy Process (AHP) to evaluate cyber risk under quantum uncertainty [15]. This approach brings interpretability and multi-criteria decision-making, but its reliance on subjective inputs and fuzzy pairwise comparisons introduces inconsistencies when applied across large organizations.

Baseri et al. presented a comprehensive framework for analyzing how quantum computing may compromise digital infrastructure [16]. Their work includes high-level architectural vulnerabilities and migration scenarios, with qualitative indicators of exposure and readiness. However, their approach lacks a quantitative scoring model, making it difficult to prioritise assets or justify phased investments. QARS addresses this by delivering a concrete, adjustable score from 0 to 1 (or 0–100).

Aslam in their work [17] conducted an exhaustive survey of quantum threats to cryptographic primitives and outlined a matrix of countermeasures. While rich in content, the paper is predominantly descriptive and lacks a prescriptive risk model that organisations can operationalise. It does not provide quantitative ranking of assets or integration into risk governance tools like QARS.

Kezron in the paper [18] focused on post-quantum readiness in U.S. community banks, proposing a checklist-style framework to assess gaps in awareness, inventory, and controls. While practical, this model remains sector-locked and lacks dimensional weighting or generalisability across other industries.

Halak et al. proposed a quantum security assessment tool that scores systems based on their quantum resistance using predefined risk vectors [19]. Although similar in aim to QARS, the model lacks continuous scaling functions and adjustable weighting. It also omits the dynamic timeline modelling that is core to QARS's extension of Mosca's inequality.

Adapa in the study [20] outlined a framework for transitioning to PQC, structured around architectural planning and cryptographic inventory. The paper emphasises strategy over scoring, and although it provides a roadmap, it lacks a numerical risk model that can assist in triaging migration based on urgency and impact. QARS complements such frameworks by offering a scoring core to inform these strategic plans.

Industry organisations and standards bodies have contributed significantly to formalising QRA methodologies. GSMA's 2023 Quantum Cryptanalytic Risk Assessment (QCRA) provides guidelines for telecom sectors, incorporating cryptographic profiling and migration prioritisation strategies. Complementing this, the World Economic Forum's Quantum Readiness Toolkit [21] offers a practical self-assessment framework emphasising cryptographic lifespan and migration readiness. NIST's guidance on post-quantum transition [22] and the forthcoming FIPS 203-205 standards outline technical requirements for quantum-safe cryptographic modules. Together, these contributions provide the technical and regulatory scaffolding required for institutional quantum risk planning.

A parallel stream of research addresses data sensitivity and adversarial exposure as critical components of quantum risk. Kumar [23] emphasises that high-sensitivity assets—particularly those under regulatory regimes such as GDPR [24] or HIPAA—require enhanced modelling in risk scoring algorithms. Exposure is also quantified through cryptographic visibility (e.g., RSA/ECC usage) and operational harvestability, including network transmission vectors and cloud-based storage risks. These dimensions are typically underrepresented in classical risk matrices but are essential in "harvest now, decrypt later" scenarios.

Cloud-specific quantum risk models have recently begun to emerge. A 2025 research initiative in [25] presents a migration assessment model for hybrid and public cloud environments, accounting for multi-tenancy, workload mobility, and key management decentralisation. The model integrates timeline, sensitivity, and exposure assessments with deployment-specific risk vectors, offering tailored recommendations for quantum-secure transitions in distributed architectures.

On the other hand, practical tooling and commercial services are gaining traction. Vendors such as evolutionQ and AvinyaSQ offer proprietary QRA platforms, integrating asset classification, cryptographic inventory, and scenario-based risk modelling [26,27]. Although these tools are not publicly validated, they demonstrate market demand for actionable, executive-facing quantum readiness dashboards. Importantly, such solutions reinforce the importance of translating theoretical risk models into operational decision support systems.

Contemporary literature increasingly converges on the need for multi-dimensional, calibrated, and context-aware models. While most models build on Mosca's inequality and the foundational triplet (X, Y, Z), they differ in scope, granularity, and operational readiness (see Table 1). The QARS model proposed in this paper seeks to unify these strands by providing a continuous, weight-adjustable risk score aligned with both theoretical constructs and evolving regulatory demands.

Table 1. Comparative overview of the analysed references.

Ref.	Proposed Solution	Risk Dimensions (T/S/E) *	Scoring Approach	Quantitative Output	Sector Adaptability	Regulatory Alignment
[9]	Timeline-based metrics	T	Timeline formula	yes	yes	partially
[10]	FS-ISAC PQC model	T, S	Maturity model	no	no	yes
[11]	STRIDE evaluation model	T, S, E	Qualitative risk matrix	no	yes	partially
[12]	QUASAR framework	T, S, E	Strategic mapping	no	yes	yes
[13]	Public health quantum model	T (indirect)	Probabilistic	no	no	no
[14]	Quantum algorithmic VaR/CVaR	T	Quantum algorithmic	yes	no	no
[15]	Fuzzy AHP	S, E	Fuzzy logic (AHP)	partially	partially	partially
[16]	Cyber infra risk framework	T, Arch.	Qualitative	no	yes	partially
[17]	Crypto threat taxonomy	T, S	Descriptive mapping	no	yes	yes
[18]	SME readiness checklist	S, Inventory	Checklist	no	no	yes
[19]	Quantum threat score tool	Resistance vectors	Static scoring	yes	yes	partially
[20]	PQC migration strategy	T, S	Strategic planning	no	yes	yes
[21]	Quantum readiness toolkit	T, S	Checklist/ Self-assessment	no	yes	yes
[22]	NIST IR 8547 draft	T	Guidance	no	yes	yes
[23]	Sensitivity/exposure profiling	S, E	Heuristic model	no	yes	yes
[25]	Cloud migration risk model	T, S, E	Composite	yes	yes	partially
[26]	EvolutionQ QRA tool	T, S, E	Proprietary scoring	yes	yes	yes
[27]	AvinyaSQ platform	T, S, E	Proprietary scoring	yes	yes	yes
-	**QARS (our model)**	**T, S, E**	**Weighted composite**	**yes**	**yes**	**yes**

* T—Timeline to compromise (e.g., X, Y, Z model); S—Sensitivity of data or asset; E—Exposure/harvestability of cryptographic material.

3. QARS Model and Method for Calibration and Sector-Specific Adaptation

3.1. QARS Model Formulation

QARS is structured on the foundation of classical risk assessment principles, where risk is expressed as a combination of likelihood and impact. This familiar framework is extended with quantum-specific threat attributes—including the quantum threat horizon, migration time, and harvestability factors—allowing direct integration with existing enterprise risk methodologies. In doing so, QARS maintains compatibility with classical risk registers while introducing parameters tailored to quantify quantum-enabled threats.

At the heart of QARS lies an extension of Mosca's triplet (X, Y, Z), which includes security shelf-life, migration time, and quantum collapse time [28], into a continuous, multi-factor risk score. For a given asset a, we define Quantum-Adjusted Risk Score by the following equation (Equation (2))

$$\mathrm{QARS}(a) \;=\; w_T\, T(a) \;+\; w_S\, S(a) \;+\; w_E\, E(a), \tag{2}$$

with non-negative weights w_T, w_S, w_E satisfying $w_T + w_S + w_E = 1$ when a $[0, 1]$ normalisation is desired. Each factor maps raw inputs into the unit interval via scaling functions described below.

(1) Timeline Risk T.

Let $X(a)$ be the required confidentiality duration (shelf-life), $Y(a)$ be the time to complete a PQC migration (mitigation window), and $Z(a)$ be the projected time until an adversary obtains a CRQC capable of breaking the asset's cryptographic primitive (threat horizon). Mosca's inequality (1) $X + Y > Z$ indicates a binary failure condition. We convert it into a real-valued metric by defining (Equation (3)):

$$r(a) \;=\; \frac{X(a) + Y(a)}{Z(a)}, \tag{3}$$

and applying a monotone scaling $f_{\mathrm{time}} : \mathbb{R}_{\geq 0} \to [0, 1]$, as seen in Equation (4):

$$T(a) \;=\; f_{\mathrm{time}}\big(r(a)\big) \;=\; \frac{1}{1 + e^{-\alpha\,(r(a)-1)}}, \tag{4}$$

where $\alpha > 0$ controls the steepness. A simpler linear surrogate $f_{\mathrm{time}}(r) = \min(1, r)$ may be used in low-uncertainty settings. Intuitively, $T(a)$ grows as the window of vulnerability between today and successful migration widens.

(2) Sensitivity Risk S.

Data and service criticality vary widely between assets. We map an organisational sensitivity label $D(a) \in \{\mathrm{Low}, \mathrm{Moderate}, \mathrm{High}, \mathrm{Critical}\}$ to a numeric score via $g : D \to [0, 1]$, e.g., $g(\mathrm{Low}) = 0.25$, $g(\mathrm{Critical}) = 1$. A scaling f_{sens} (typically identity) yields Equation (5):

$$S(a) \;=\; f_{\mathrm{sens}}\big(g(D(a))\big). \tag{5}$$

Long-lived secrecy requirements can be encoded either by elevating $X(a)$ in (3) or by mapping $D(a) \to \mathrm{Critical}$, thereby reflecting regulatory mandates (e.g., GDPR, HIPAA) in the impact dimension [29].

(3) Exposure Risk E.

Exposure combines cryptographic and operational visibility (see Equations (6)–(8)):

$$v(a) = \begin{cases} 1, & \text{if RSA/ECC/DH in use,} \\ 0, & \text{if PQC or non-public-key primitive,} \end{cases} \tag{6}$$

$$q(a) \in [0, 1] \quad \text{(network / cloud / supply-chain harvestability),} \tag{7}$$

$$E(a) = f_{\mathrm{expos}}\big(v(a), q(a)\big) = v(a)\, q(a), \tag{8}$$

so that PQC-protected assets ($v = 0$) are assigned $E = 0$. The function f_{expos} may incorporate sectoral compliance multipliers (e.g., stricter weights for NIS 2 entities).

While the current formulation uses a binary cryptographic visibility factor $v(a)$ and a single harvestability score $q(a)$ for clarity, this structure is intentionally modular and can be refined for more nuanced threat modelling. Future iterations of QARS will replace $v(a)$ with a graded cryptographic visibility scale that accounts for factors such as forward secrecy, hybrid PQC–classical schemes, and partial key exposure scenarios (e.g., TLS session key compromise). Likewise, $q(a)$ will be expanded into sub-factors reflecting interception potential, data persistence, and susceptibility to implementation-level attacks such as timing or electromagnetic side channels.

All three scaling functions $f_{\text{time}}, f_{\text{sens}}, f_{\text{expos}}$ should be documented and, where possible, harmonised with industry benchmarks. Piece-wise linear or logistic maps are recommended for interpretability. Assets thus receive QARS $\in [0,1]$ (or scaled to $[0,100]$) enabling direct ranking by quantum urgency and severity.

3.2. Design Motivations

The structure of the QARS model is not arbitrary: each dimension such as a timeline risk (T), sensitivity risk (S), and exposure risk (E) was deliberately chosen to address specific limitations in existing quantum risk assessment approaches. The objective was to build a composite risk scoring model that is both operationally useful and theoretically grounded, enabling organizations to prioritize post-quantum migration in a nuanced, evidence-based manner.

Without T, a risk model cannot distinguish assets whose security lifetime clearly exceeds the CRQC horizon. EU roadmap guidance classifies any use case demanding confidentiality beyond 2030 as a "high-risk" [1]. T is explicitly engineered to flag such cases. While time defines when a threat becomes viable, sensitivity defines the consequences if the threat materialises. Not all data is equally important: a compromised internal log file may be trivial, while exposure of medical records or state secrets may result in legal, financial, or even geopolitical damage.

The S dimension maps qualitative sensitivity labels to numeric scores, ensuring that impact severity is embedded into the final risk index. This reflects both technical value and regulatory importance: for instance, datasets governed by GDPR or HIPAA must retain confidentiality beyond minimum thresholds, often implying high long-term impact. Embedding sensitivity into the model prevents over-prioritisation of systems that may be technically vulnerable but operationally insignificant. It also ensures compliance requirements are directly factored into the risk calculus, avoiding reliance on external audits or human memory to flag sensitive assets.

Even highly sensitive assets may pose minimal risk if they are well isolated or protected by PQC primitives. Conversely, a trivial system using classical RSA over a public network may be harvested today and decrypted later, forming a high-risk "harvest-now, decrypt-later" scenario. The E component of QARS addresses this by combining cryptographic visibility (e.g., whether the asset still uses breakable algorithms) with operational harvestability factors such as internet exposure, use of cloud services, or third-party API integration. This ensures that even technically secure-looking systems can be flagged if their ciphertext is likely to be intercepted and stored. This dimension fills a critical gap in existing models, which often focus on impact but fail to quantify exploitability. Including E ensures that QARS does not over-rely on hypothetical worst-case scenarios but remains anchored in real-world adversarial capabilities.

Together, the triad yields a balanced, unified metric akin to classical *Risk* = *Probability* × *Impact*, but tailored to quantum conditions. Instead of relying on black-box scoring, security professionals and stakeholders can see precisely why a given system is scored highly and which mitigation strategies (e.g., shortening Y, switching to PQC, isolating data) would most effectively reduce the QARS score.

3.3. Calibration Method and Sector-Specific Weights

The QARS model is designed to be flexible and adaptable across sectors with varying risk tolerances, regulatory requirements, and asset profiles. To achieve meaningful and actionable scores, careful calibration is essential. Calibration ensures that the scoring reflects realistic urgency levels and that QARS outputs are aligned with institutional risk management priorities (Figure 1).

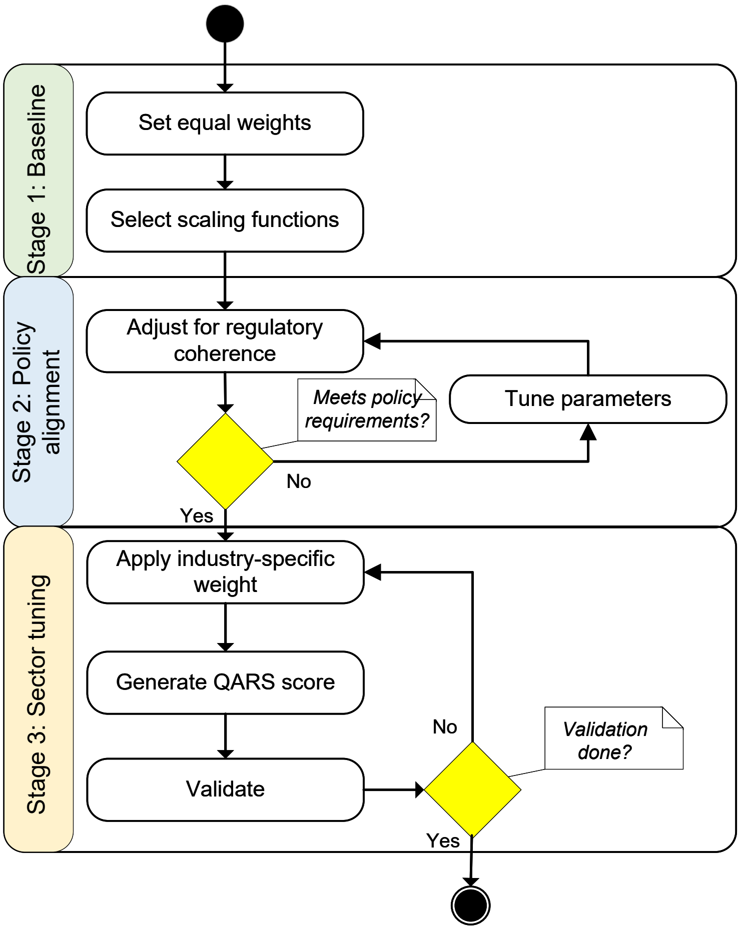


Figure 1. The flowchart of the calibration method.

This process unfolds in three stages:

1. Baseline: Initialise $w_T = w_S = w_E = \frac{1}{3}$ to give equal importance to all three risk dimensions in the absence of sector-specific guidance. Scaling functions for T, S, and E such as logistic or piecewise linear maps are selected so that typical asset parameters produce values spanning the full unit interval $[0,1]$. This guarantees numerical differentiation between low-, medium-, and high-risk assets. For example, timeline scaling $f_{\text{time}}(r)$ can be tuned so that $r = 1$ corresponds to a neutral score of 0.5, while higher r values push T closer to 1.
2. Policy alignment: To ensure regulatory coherence, weights and scaling functions are adjusted so that assets already deemed "high-risk" by institutional or governmental guidance exceed a given QARS threshold. For instance, if regulators require quantum safety for any system with $X > 10$ years and $Z = 8$, the model should yield QARS > 0.70 for such configurations. This alignment anchors QARS to existing compliance frameworks like the EU PQC Roadmap, NIS 2, or sector-specific advisories.

In practice, model designers may tune α in the logistic scaling or elevate sensitivity mappings (e.g., Critical $\mapsto$ 1.0) to meet these constraints.

3. Sector tuning: Different industries have distinct quantum risk exposure profiles and risk appetites. Sector-specific weighting profiles enable QARS to reflect these nuances in the following examples:
    - In finance, where confidentiality and regulatory compliance are paramount, a typical profile is $(w_T, w_S, w_E) = (0.4, 0.4, 0.2)$, prioritising long-term protection and impact severity.
    - In Internet-of-Things (IoT) or embedded systems, the threat is often driven more by constrained upgrade cycles and wide exposure surfaces; thus $(w_T, w_S, w_E) = (0.5, 0.2, 0.3)$ may be more appropriate.
    - In cloud-native services, where exposure to data harvesting is high, an organisation may increase w_E accordingly, e.g., $(0.3, 0.2, 0.5)$.

    Scaling functions may also be adjusted at this stage: a highly risk-averse sector might use steeper curves (e.g., higher α in the logistic function) to emphasise high-risk regions, whereas a sector under resource constraints may smooth the gradient to avoid excessive migration clustering.

This multi-phase calibration allows QARS to function as both a universal and domain-sensitive framework. Baseline values ensure comparability across institutions, policy alignment ties scores to compliance requirements, and sector tuning enables prioritization strategies tailored to practical needs. Through these adjustments, QARS becomes a living model that evolves with organisational context, regulatory updates, and technological change.

3.4. Validation Strategy

Because no real-world data yet exist on "successful quantum hacks", we check that QARS behaves sensibly in four practical ways. Cryptography specialists and CISOs inspect QARS results for a selection of systems. To expand on this process, expert validation begins with structured walkthroughs involving key stakeholders, such as information security officers, cryptographic engineers, and compliance leads. These professionals are presented with anonymised QARS outputs alongside system descriptions and asked whether the scores align with their intuitive and regulatory expectations. Significant mismatches trigger a review of weightings or scaling logic, ensuring that human expertise remains embedded in the refinement loop. If their professional judgement and the score disagree, we fine-tune the model's factors.

Second, hypothetical scenarios are not chosen at random but are systematically constructed to cover edge cases such as assets with low sensitivity but high exposure, or systems with strong encryption but long migration timelines. We invent hypothetical cases, such as a system that must stay secret for 30 years versus one that matters for only 1 year and confirm that QARS ranks the long-term system much higher. These synthetic profiles help stress-test the model's consistency and identify any nonlinearities or distortions in the scoring behaviour. In some cases, organisations simulate legacy versus greenfield deployments to examine how architectural changes influence QARS.

Third, we place QARS values next to the scores from CARAF and Mosca's original, simpler model. A comparative testing with CARAF and Mosca-based models is conducted using paired scoring exercises, where QARS is calculated alongside the alternative models for a fixed set of assets. Analysts then evaluate whether QARS preserves the ordinal relationships while providing additional explanatory power. These comparisons are useful not only for validation but also for change management, as organisations transition from qualitative checklists to quantitative scoring tools.

Fourth, the Streamlit prototype serves as a human-in-the-loop feedback tool. A small Streamlit web app lets organisations enter their own data and see the live score. User feedback on whether the number "feels right" feeds back into further tweaks. It is designed not just to calculate scores, but to prompt users with reflection questions like "Does this ranking surprise you?" or "Would you assign a higher priority to this asset based on business impact?" Answers are logged (with user consent) and reviewed in calibration workshops. This participatory loop transforms QARS from a static model into a continuously evolving decision support system.

These checks are repeated on a regular basis, especially as post-quantum pilot projects complete and new estimates for the "quantum-attack date" appear from bodies such as the Global Risk Institute or NIST to keep QARS up to date.

In this way, QARS model is subjected to periodic validation cycles, analogous to model governance practices in financial risk modelling. Organisations are encouraged to re-run the validation suite annually or when material changes occur such as the adoption of PQC primitives, introduction of new data flows, or publication of revised quantum readiness timelines.

Continuous re-validation is planned as PQC pilots mature and the quantum threat timeline is periodically updated by responsible bodies (e.g., Global Risk Institute and NIST).

4. Empirical Results and Model Demonstration

To evaluate the practical utility and interpretability of the QARS model, this section presents a series of illustrative examples, comparative analyses, and early-stage user feedback. Because real-world data on quantum-compromised systems do not yet exist, our approach relies on carefully constructed hypothetical cases, expert review, and consistency checks with existing frameworks such as Mosca's inequality and CARAF.

The primary goal is to demonstrate that QARS produces results that align with expert intuition, regulatory expectations, and operational realities, while also offering greater granularity and flexibility than binary or rule-based methods. We also showcase a lightweight, interactive prototype that allows organisations to test QARS on their own systems and explore how variations in parameters (e.g., timeline, sensitivity, cryptographic exposure) affect the final score.

4.1. Illustrative QARS Calculation

To show how the QARS model behaves under realistic but simplified conditions, we construct several illustrative asset profiles. Each example varies one or more parameters, such as the required confidentiality period, algorithm in use, or data classification, in order to observe how these changes affect the overall QARS score. This allows us to assess the model's responsiveness to input variation and its ability to preserve intuitive ordering. Parameter values were chosen to accentuate the difference between long-lived sensitive data and a short-lived, low-impact service. Table 2 summarises the input parameters and resulting factor scores; calculations follow Equations (2), (4), (5) and (8) with equal weights $w_T = w_S = w_E = \frac{1}{3}$.

Table 2. Illustrative assets and calculated QARS components.

Asset	X (y)	Y (y)	Z (y)	T	S	E	QARS
A: Confidential archive	15	5	12	1.00	0.90	0.30	0.733
B: Public web service	1	2	12	0.25	0.10	0.80	0.383

Example calculations for asset A: long-term confidential document storage:
Here, $X+Y = 20 > Z = 12$, producing $T \approx 1$. High sensitivity ($S = 0.9$) and modest

exposure ($E = 0.3$) yield $\text{QARS}_A = \frac{1}{3}(1.0 + 0.9 + 0.3) \approx 0.73$, placing the asset firmly in the high-risk band. A finance sector weight set $(w_T, w_S, w_E) = (0.4, 0.4, 0.2)$ would push $\text{QARS}_A \approx 0.82$—approaching the critical threshold and corroborating EU guidance that such archives must be quantum-safe by 2030.
Example calculations for asset B: short-lived public web service:
With $X+Y = 3 \ll Z$, timeline risk is low ($T = 0.25$). Combined with low sensitivity ($S = 0.1$) and high exposure ($E = 0.8$) the result is $\text{QARS}_B \approx 0.38$, i.e., low–medium risk. Even though E is large, the short confidentiality horizon keeps overall risk modest; migration can occur during routine refresh cycles.

The purpose of these examples was twofold: first, to validate that the model behaves in a stable and explainable way; second, to help practitioners develop a feel for how different configurations influence quantum risk. These examples illustrate QARS's discriminative power: a long-lived, high-impact system is prioritised over a transient, low-impact service, matching expert intuition. These synthetic cases act as templates that organisations can adapt when assessing their own systems using the prototype tool introduced later.

4.2. Alignment with Qualitative Risk Categories

While QARS model produces a continuous score between 0 and 1, practical decision-making often benefits from simplified categorical guidance. To that end, we map continuous scores onto qualitative bands that classify scores into intuitive risk levels: low, medium, high, and critical. These bands offer a bridge between the quantitative output of the model and the qualitative language typically used in security governance, compliance mandates, and roadmap planning.

The thresholds for each category are informed by both expert judgement and regulatory expectations, particularly those articulated in the EU's Coordinated PQC Roadmap. This mapping allows organisations to interpret QARS results not just in absolute terms, but as indicators of migration urgency, budget prioritisation, and policy alignment.

Mapping continuous scores onto qualitative bands (low < 0.30, medium 0.30–0.60, high > 0.60, critical > 0.85) yields the following results:

- Asset A $(0.73) \rightarrow$ high,
- Asset B $(0.38) \rightarrow$ medium–low.

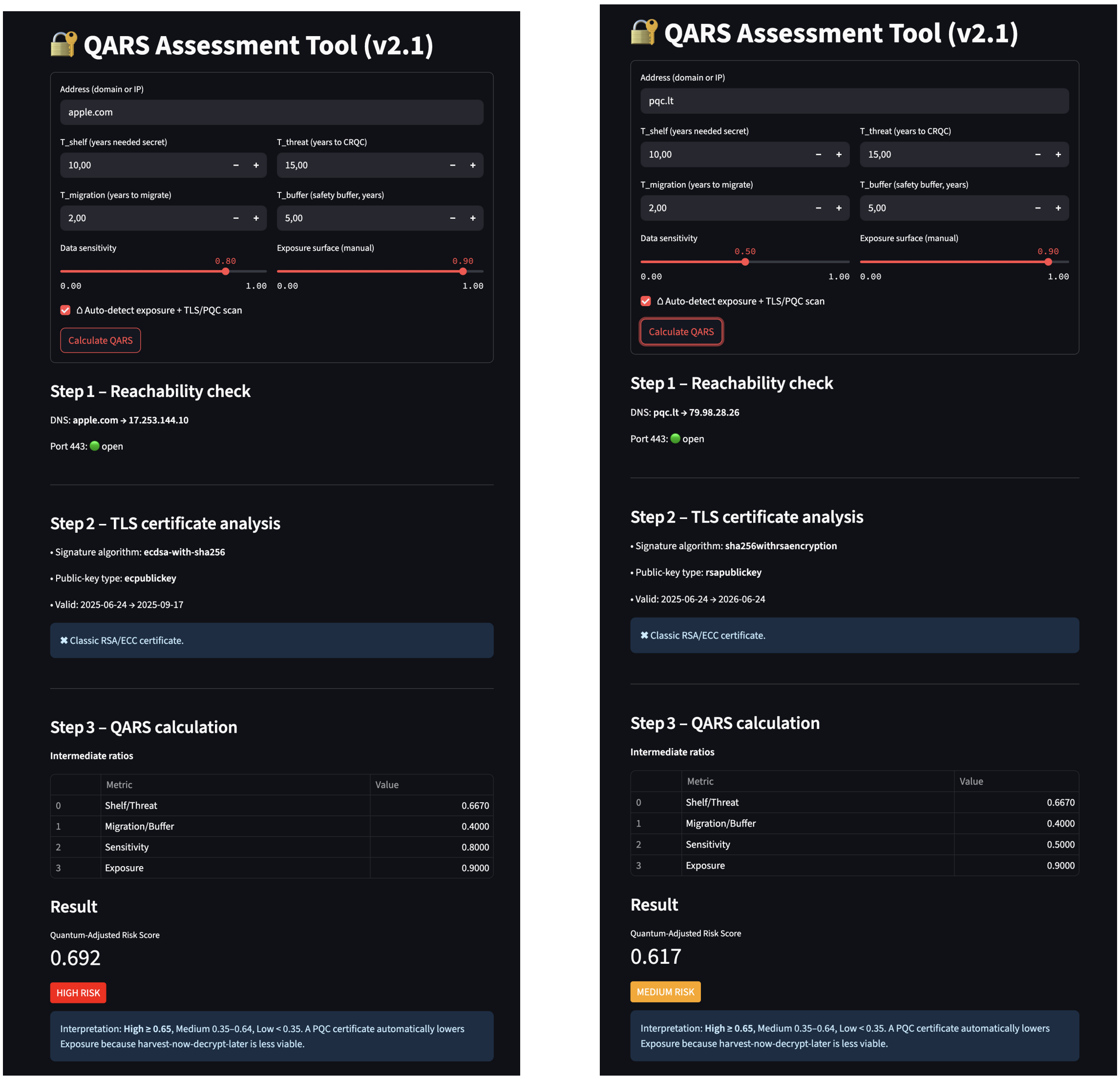
These bands mirror the EU's Coordinated PQC Roadmap, whereby high-risk systems (critical functions or $X > 10$ years) must be quantum-safe by 2030, 2035 for medium-risk, and "as feasible" for low-risk. QARS therefore provides a numerical substrate for roadmap milestones and risk-based scheduling.

Sensitivity analysis confirms responsiveness: reducing the threat horizon to $Z = 8$ instantly lifts timeline factors ($T_A \rightarrow 1$, $T_B \rightarrow 0.37$) and pushes multiple assets over the high threshold—an effect exploitable in annual re-assessments.

4.3. Prototype Tool Demonstration

To complement the theoretical QARS model and illustrative examples, we developed a lightweight prototype tool that allows users to interactively explore the QARS model. The tool, built using Streamlit, provides a browser-based interface where organisations can input the basic parameters (X, Y, Z), and select a data-sensitivity level as well as an exposure estimate. Based on these inputs, the tool instantly computes the QARS score, classifies the asset into a qualitative band, and colours the resulting QARS badge (green, amber, red). Figure 2 presents the two windows of the QARS assessment tool, where

- Asset A (left panel) is flagged high-risk in red, prompting "Begin PQC migration immediately";
- Asset B (right panel) receives an amber medium risk badge, indicating migration can be scheduled during normal maintenance.



🔐 QARS Assessment Tool (v2.1)

Address (domain or IP): apple.com

T_shelf (years needed secret): 10,00

T_threat (years to CRQC): 15,00

T_migration (years to migrate): 2,00

T_buffer (safety buffer, years): 5,00

Data sensitivity: 0.80 (0.00 – 1.00)

Exposure surface (manual): 0.90 (0.00 – 1.00)

☑ ⌂ Auto-detect exposure + TLS/PQC scan

Step 1 – Reachability check

DNS: **apple.com → 17.253.144.10**

Port 443: 🟢 open

Step 2 – TLS certificate analysis

- Signature algorithm: **ecdsa-with-sha256**
- Public-key type: **ecpublickey**
- Valid: 2025-06-24 → 2025-09-17

✖ Classic RSA/ECC certificate.

Step 3 – QARS calculation

Intermediate ratios

	Metric	Value
0	Shelf/Threat	0.6670
1	Migration/Buffer	0.4000
2	Sensitivity	0.8000
3	Exposure	0.9000

Result

Quantum-Adjusted Risk Score

0.692

HIGH RISK

Interpretation: **High ≥ 0.65**, Medium 0.35–0.64, Low < 0.35. A PQC certificate automatically lowers Exposure because harvest-now-decrypt-later is less viable.

(**a**)

🔐 QARS Assessment Tool (v2.1)

Address (domain or IP): pqc.lt

T_shelf (years needed secret): 10,00

T_threat (years to CRQC): 15,00

T_migration (years to migrate): 2,00

T_buffer (safety buffer, years): 5,00

Data sensitivity: 0.50 (0.00 – 1.00)

Exposure surface (manual): 0.90 (0.00 – 1.00)

☑ ⌂ Auto-detect exposure + TLS/PQC scan

Step 1 – Reachability check

DNS: **pqc.lt → 79.98.28.26**

Port 443: 🟢 open

Step 2 – TLS certificate analysis

- Signature algorithm: **sha256withrsaencryption**
- Public-key type: **rsapublickey**
- Valid: 2025-06-24 → 2026-06-24

✖ Classic RSA/ECC certificate.

Step 3 – QARS calculation

Intermediate ratios

	Metric	Value
0	Shelf/Threat	0.6670
1	Migration/Buffer	0.4000
2	Sensitivity	0.5000
3	Exposure	0.9000

Result

Quantum-Adjusted Risk Score

0.617

MEDIUM RISK

Interpretation: **High ≥ 0.65**, Medium 0.35–0.64, Low < 0.35. A PQC certificate automatically lowers Exposure because harvest-now-decrypt-later is less viable.

(**b**)

Figure 2. Screenshots of the QARS assessment tool: (**a**) Asset A—long-term confidential archive (QARS = 0.692; High); (**b**) Asset B—short-lived public web service (QARS = 0.617; Medium. Badge colour (red, amber, green) and headline text immediately communicate priority.)

This live interface serves several purposes. First, it offers immediate practical value for CISOs, risk managers, and systems architects seeking to prioritise post-quantum migration efforts. Second, it encourages transparency and interpretability: users can see how each component contributes to the overall score and adjust assumptions in real time. The tool acts as a feedback mechanism for model refinement. By collecting anonymised user inputs and comments (where permitted), we gain insights into whether the scores align with expert expectations and real-world prioritisation logic. Stakeholders reported that this visual feedback clarified priorities and helped them draft PQC roadmaps more quickly.

4.4. Preliminary Validation and Model Governance

Early-stage testing of the QARS model within a pilot deployment at a financial institution yielded encouraging results. Security and cryptography specialists were asked to evaluate a curated set of internal systems using their own risk assessment heuristics, and these subjective judgements were then compared to QARS outputs. In the majority of cases, the ordering produced by QARS aligned closely with expert expectations, reinforcing confidence in the model's internal logic and external face validity.

Notably, one archival storage system—historically rated as medium-priority using a qualitative risk matrix—received a substantially higher QARS score due to its exceptionally long required confidentiality duration and reliance on legacy public-key cryptography. This discrepancy prompted a re-evaluation by the internal team and led to a reprioritisation of the system for early migration. This case illustrates QARS's added value: by quantifying timeline risk and exposure in a continuous, scalable fashion, the model highlights risk patterns that are easy to miss in binary or matrix-based schemes.

In addition to internal validation, we compared QARS rankings with those generated using the fS-ISAC post-quantum risk assessment model [10]. While both models identified similar asset categories as high-risk, QARS demonstrated superior granularity within categories, enabling decision-makers to rank assets not just by type but by the specific configuration of timeline, sensitivity, and exposure parameters. This intra-category differentiation is critical in practice, particularly when budgetary or resource constraints demand phased rather than bulk migrations.

To assess numerical robustness, we also conducted a sensitivity analysis in which input parameters (e.g., projected quantum timeline Z, asset lifespan X, or cryptographic visibility) were systematically varied. QARS responses were continuous and stable under small perturbations and appropriately reactive under larger shifts—indicating that the model is neither overly rigid nor overly volatile. These numerical characteristics support its suitability for use in annual reassessments and rolling risk-adjustment strategies.

In addition to alignment with expert intuition, QARS demonstrated governance and explainability capabilities that are essential for regulatory acceptance in sectors such as finance, healthcare, and critical infrastructure. For each scored asset, the model stores input parameters $(X, Y, Z, D(a), v(a), q(a))$, scaling functions, and weight settings in a scenario log, enabling full reproducibility of results. The prototype tool offers a decomposition view, showing the contribution of timeline risk $T(a)$, sensitivity risk $S(a)$, and exposure risk $E(a)$ to the final score, as well as parameter sensitivity analysis to simulate mitigation effects (e.g., reduced migration time or adoption of hybrid PQC–classical schemes). QARS outputs can be exported into governance, risk, and compliance (GRC) platforms with metadata on scoring date, responsible analyst, and mitigation status, facilitating audit readiness. By embedding traceability, explainability, and audit integration features into the QARS framework, the model supports both operational decision-making and compliance with emerging transparency requirements for algorithmic risk scoring. These governance measures, combined with expert validation and comparative testing against existing frameworks, enhance confidence in QARS's readiness for adoption in high-assurance environments.

Initial evidence suggests QARS outputs are both comprehensive, covering all salient quantum risk facets, and actionable, translating directly into phased mitigation plans. Further large-scale validation is planned as additional sector pilots commence.

5. Discussion

The proposed QARS model advances quantum cybersecurity risk assessment by furnishing a unified, quantitative metric that aggregates multiple risk dimensions. Prior frameworks either isolated the timeline factor [28] or treated crypto-agility in qualitative check-lists [5]. QARS instead fuses when the threat materialises (timeline), what the impact is (sensitivity), and how adversaries can exploit the asset (exposure), mirroring the classical Risk = Likelihood × Impact equation in a quantum context. By extending Mosca's (X, Y, Z) triplet to the multi-factor score (see Equation (2)), QARS overcomes criticisms that Mosca's theorem is too coarse for operational decision-making (e.g., [29]). Industry white papers have hinted at “multi-parameter” extensions of Mosca’s model; QARS supplies a concrete instantiation.

Although QARS is not a direct probability, it may be viewed as a dimensionless index proportional to

$$\underbrace{w_T\, P\big(\text{CRQC arrives before migration}\big)}_{\text{timeline-driven likelihood}} + \underbrace{w_E\, P\big(\text{data exposure}\big)}_{\text{exposure-driven likelihood}} + \underbrace{w_S\, \text{Impact}}_{\text{consequence}},$$

where $T = 1$ approximates certainty of pre-migration quantum break and, similarly, E scales with harvest probability. A formal Bayesian interpretation is left to future work, pending better empirical priors on Z.

QARS is designed for seamless insertion into existing governance structures. Each asset receives a QARS field (e.g., “System A—QARS 0.75 (high)—mitigate by 20XX”), enabling quantitative comparison with other cyber risks and allowing post-mitigation re-scoring to demonstrate risk reduction. Implementing hybrid TLS or a PQC VPN sets $v\downarrow$ and hence $E\downarrow$, instantly lowering QARS—useful for cost–benefit analysis under CARAF’s timeline × cost heuristic. In the PAREK lifecycle, QARS feeds the road-map stage: assets are sorted by score, highest first, aligning with EU recommendations for phased migration [1]. QARS model supplies likelihood/impact numbers that can be embedded in FAIR or NIST 800-30 registers, ensuring quantum risk is evaluated alongside classical threats rather than siloed.

The QARS model aligns closely with emerging regulatory mandates and offers a practical methodology for implementing risk-based, post-quantum migration strategies. Specifically, it provides immediate support for the EU’s 2025 Coordinated Roadmap, facilitating Milestone 1 (completion of a quantum risk inventory by 2026) and enabling subsequent system prioritisation through its scalar outputs. These quantitative scores enhance executive-level communication by allowing concise summaries such as “15 systems with QARS > 0.8 must be migrated by 2030.” While the NIS 2 Directive does not explicitly reference quantum threats, it mandates continuous risk assessments that account for emerging technologies; QARS can serve as a harmonised scoring standard, enabling regulators to request, for example, “a list of the top five QARS-ranked assets and their planned mitigation timelines” in compliance submissions. Similarly, the Cyber Resilience Act (CRA) [8], through its secure-by-design mandate and forthcoming cryptographic agility requirements, is well-aligned with QARS principles. A product line exceeding a QARS score of 0.8, indicating high cryptographic exposure and long-term sensitivity, would likely fall short of CRA expectations unless it demonstrates post-quantum upgradeability, making QARS a defensible justification for integrating PQC readiness into product design.

Beyond the EU, QARS is positioned for applicability within global regulatory and standardisation efforts. In the United States, the National Security Memorandum 10 (NSM-10) [30] and related guidance from the Cybersecurity and Infrastructure Security Agency (CISA) emphasise cryptographic asset inventory, migration prioritisation, and risk-based scheduling—objectives directly supported by QARS’s quantitative scoring. The model’s modular T–S–E structure is also compatible with the ongoing work of ISO/IEC crypto-agility working groups, which seek standardised approaches for algorithm agility, risk assessment, and migration planning. Furthermore, QARS can be integrated with frameworks promoted by other global bodies, such as the World Economic Forum’s Quantum Readiness Toolkit, ensuring that transnational organisations operating across multiple jurisdictions can adopt a harmonised, standards-aware methodology for quantum risk assessment.

5.1. Comparison with Related Work

Several existing approaches to quantum risk assessment such as Mosca's early framework and sectoral models like those used in financial services rely on categorical scoring schemes, typically assigning integer levels (e.g., 1–4) to input parameters such as the required confidentiality duration (X), estimated migration time (Y), and projected quantum-breaking horizon (Z). In contrast, QARS model introduces a continuous scoring approach that captures more nuanced differences between assets, allowing for smoother prioritisation across a wider range of system profiles. Moreover, QARS extends beyond timeline considerations by explicitly incorporating two additional dimensions: the sensitivity, which captures the business or regulatory impact of compromise, and the exposure, which quantifies the likelihood of ciphertext interception and potential misuse. Despite this added complexity, QARS remains compatible with the intuitive labels used in earlier models; for example, thresholds such as QARS > 0.8 can map to "critical" and the range 0.5–0.8 to "high," preserving the interpretability of earlier qualitative taxonomies.

Previous quantitative formulations often express quantum risk as a product of timeline urgency and anticipated remediation cost (e.g., Risk = Timeline × Cost). QARS generalises this structure in two key ways. First, it decomposes the notion of "cost" into explicit sensitivity (S), reflecting the severity of impact, and exposure (E), capturing threat surface and cryptographic visibility, thereby offering a more semantically grounded representation of risk components. Second, QARS introduces sector-specific weighting capabilities, allowing different domains (e.g., finance, IoT, government) to adjust the relative emphasis on each component according to their operational priorities or regulatory context. Additionally, the model offers visibility into cryptographic agility: as organisations reduce migration timelines ($Y \downarrow$) and modernise key infrastructure, the resulting decrease in timeline factor (T) is immediately reflected in a lower overall QARS score. This real-time feedback loop makes QARS suitable not only for snapshot risk assessments but also for tracking progress across post-quantum readiness initiatives.

5.2. Limitations and Future Work

The effectiveness and reliability of the QARS model are inherently dependent on assumptions regarding the arrival timeline of cryptographically relevant quantum computers (CRQC). Given the uncertainty surrounding this parameter, regular scenario analysis and annual updates to model inputs, particularly the estimated quantum horizon (q), migration effort (Y), and sensitivity classifications are recommended. These inputs currently require expert judgement and may vary across organisations; however, the adoption of standardised classification criteria and the use of automated discovery tools (e.g., cryptographic asset scanners) could mitigate inter-operator variability and enhance reproducibility. As a point-in-time scoring model, QARS does not automatically reflect changes in system state or threat conditions; thus, effective integration into change-management workflows is necessary to ensure recalculation is triggered upon upgrades, exposure events, or algorithmic shifts. Additionally, the present version of QARS focuses primarily on confidentiality risks associated with public-key cryptosystems; integrity risks, such as those stemming from quantum-enabled signature forgery, are not yet explicitly modelled. Future extensions will seek to adapt the framework to cover integrity-sensitive use cases, such as software signing, digital identity, and blockchain consensus protocols.

While QARS in its current form is optimised for assessing the confidentiality risks posed by quantum algorithms targeting classical public-key cryptosystems, the model is designed to be extensible. Future work will adapt QARS to encompass other quantum attack modalities, including entanglement-based interception, quantum man-in-the-middle threats to QKD infrastructures, and quantum side-channel exploitation. These will be represented through additional exposure vectors or dedicated weighting factors, enabling the model to capture a wider spectrum of quantum threats without losing its continuous scoring structure.

Further research will aim to enhance the empirical grounding of the model. In particular, the collection of real-world migration times and incident data related to cryptographic exposure will allow for refinement of the scaling functions and calibration of sector-specific weights. This will reduce reliance on synthetic scenarios and subjective expert judgement, thereby increasing the model's generalisability and operational readiness. Integration of QARS into governance, risk, and compliance platforms would support continuous monitoring, while the development of stochastic modules such as Monte Carlo simulations of the quantum threat timeline could enable probabilistic risk outputs in place of deterministic scores. Planned cross-sector pilots will benchmark QARS against legacy matrix-based approaches and may reveal patterns of risk concentration through anonymised aggregate analyses.

Additional development will also explore QARS adaptations to other quantum-relevant domains, including systems vulnerable to Grover-type symmetric key attacks and hybrid use cases where quantum technologies themselves introduce novel security challenges. As such, QARS is intended to function as a dynamic and extensible model, capable of evolving in step with the global post-quantum cryptography transition and the continuously shifting quantum threat landscape.

6. Conclusions

This paper has introduced a unified quantum risk assessment, presenting QARS as a comprehensive model for quantifying the risk that quantum computing poses to existing cryptographic systems. By extending Mosca's inequality from a binary condition to a continuous, multi-factor score, QARS captures three essential dimensions—timeline, sensitivity and exposure. The formal definitions and weighting scheme show how these factors combine into a single, communicable metric that enables clear prioritisation of PQC migration.

The inclusion of all three dimensions guarantees that the key questions such as "When can a quantum break occur? What is the consequence? How likely is exploitation?" are simultaneously addressed. Calibration levers and sector-specific weight profiles render the QARS model adaptable from finance to IoT, acknowledging that quantum risk is not uniform across domains.

By embedding the QARS model within the EU PAREK framework, we have placed the model in a broader policy context. The EU's Coordinated PQC Roadmap, NIS 2 and the forthcoming CRA all call for an urgent yet risk-based transition to quantum-safe security. The proposed QARS model operationalises that call, helping stakeholders identify which systems to upgrade first and providing a quantitative basis for investment decisions. The prototype Streamlit tool demonstrates that QARS is readily usable: organisations can track risk trajectories in real time and verify that mitigations produce measurable score reductions.

Illustrative case studies and preliminary validations indicate that the QARS model aligns with expert judgements and policy classifications, offering more nuance than binary rules and thus finer prioritisation. We stress that QARS augments rather than replaces human expertise; it supplies the quantitative evidence that boards, regulators, and engineers need to justify immediate action on critical systems.

As the quantum era approaches, solutions like our proposed QARS model will be vital for efficient resource allocation and for safeguarding the integrity of digital infrastructure. We invite continued adoption and critique of the QARS model by both academia and industry, and plan to refine the model through additional pilot studies, automation, and integration with international standards bodies. A unified quantum risk assessment, as exemplified by QARS, will be essential to building collective resilience against the impending quantum cryptographic threat.

Author Contributions: Conceptualisation, Š.G.; methodology, R.B.; software, Š.G.; validation, Š.G. and R.B.; formal analysis, R.B.; investigation, Š.G. and R.B.; resources, Š.G.; data curation, Š.G.; writing—original draft preparation, Š.G.; writing—review and editing, R.B.; visualisation, Š.G. and R.B.; supervision, Š.G.; project administration, Š.G.; funding acquisition, Š.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was conducted as part of the execution of Project “Mission-driven Implementation of Science and Innovation Programmes” (No. 02-002-P-0001), funded by the Economic Revitalization and Resilience Enhancement Plan “New Generation Lithuania”.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this paper are available on request from the corresponding author. The incompleteness of the project prevents the data from being publicly available.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. NIS Cooperation Group. *A Coordinated Implementation Roadmap to Transition to PQC—Part 1*; Technical report; Publications Office of the European Union: Luxembourg, 2025.
2. Gidney, C. How to factor 2048 bit RSA integers with less than a million noisy qubits. *arXiv* **2025**, arXiv:2505.15917. [CrossRef]
3. Mosca, M. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
4. Piani, M.; Mosca, M. *Quantum Threat Timeline Report (2023)*; Global Risk Institute: Toronto, ON, Canada, 2023.
5. Ma, C.; Colon, L.; Dera, J.; Rashidi, B.; Garg, V. CARAF: Crypto agility risk assessment framework. *J. Cybersecur.* **2021**, *7*, tyab013. [CrossRef]
6. European Commission. *Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*; Commission Recommendation (EU) 2024/1101 C(2024) 2393 Final; European Commission, Directorate-General for Communications Networks, Content and Technology: Brussels, Belgium, 2024. Available online: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography (accessed on 11 July 2025).
7. European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS 2). *Off. J. Eur. Union* **2022**, *L333*, 80–152.
8. European Parliament and Council of the European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). *Off. J. Eur. Union* **2024**, *L2847*. Available online: http://data.europa.eu/eli/reg/2024/2847/oj (accessed on 11 July 2025).
9. Kumar, G. Timeline Risk Analysis in Quantum Risk Management. *LinkedIn Pulse*, May 2025. Available online: https://www.linkedin.com/pulse/timeline-risk-analysis-quantum-management-gireesh-kumar-n-va8jc/ (accessed on 3 July 2025).
10. FS-ISAC PQC Working Group. *Post-Quantum Cryptography Risk Model*; Technical report; FS-ISAC: Reston, VA, USA, 2023. Available online: https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf (accessed on 30 June 2025).
11. Baseri, Y.; Chouhan, V.; Ghorbani, A.; Chow, A. Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. *Comput. Secur.* **2025**, *150*, 104272. [CrossRef]
12. Weinberg, A.I. Preparing for the Post Quantum Era: Quantum Ready Architecture for Security and Risk Management (QUASAR)–A Strategic Framework for Cybersecurity. *arXiv* **2025**, arXiv:2505.17034.
13. Yang, J.; Wang, P.; Zhang, Y.; Cai, D.; Huo, Z.; Meng, H.; Shi, C.; Duan, Y.; Zhu, Q. A Quantum Model for Risk Assessment of Public Health Emergencies. In Proceedings of the International Conference on Computer Engineering and Networks, Kashi, China, 18–21 October 2024; Springer: Berlin/Heidelberg, Germany, 2024; pp. 25–32.
14. Woerner, S.; Egger, D.J. Quantum risk analysis. *npj Quantum Inf.* **2019**, *5*, 15. [CrossRef]
15. Ahmad, M.; Fatima, E.; Shukla, A.; Bhusal, N.; Khaliq, M.; Agrawal, A. Quantum Security in Cyber Risk Analysis Through Fuzzy Analytic Hierarchy Process. *J. Inf. Secur. Cybercrimes Res. (JISCR)* **2024**, *7*, 143–155. [CrossRef]

16. Baseri, Y.; Chouhan, V.; Ghorbani, A. Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. *arXiv* **2024**, arXiv:2404.10659. [CrossRef]
17. Aslam, A. Quantum Computing Threats to Cryptography: A Comprehensive Analysis of Vulnerabilities, Countermeasures, and Future-Proofing Strategies. *Preprint* **2025**. [CrossRef]
18. Kezron, I.E. Post-quantum cryptography readiness in us community banks and financial smes: A cybersecurity risk assessment framework. *Well Test. J.* **2025**, *34*, 135–146.
19. Halak, B.; Csete, C.S.; Joyce, E.; Papaioannou, J.; Pires, A.; Soma, J.; Gokkaya, B.; Murphy, M. A security assessment tool for quantum threat analysis. *arXiv* **2024**, arXiv:2407.13523. [CrossRef]
20. Adapa, V.R.K. Architecting quantum-resistant cybersecurity: A framework for transitioning to post-quantum cryptographic systems. *Int. J. Sci. Res. Arch.* **2025**, *14*, 737–746.
21. World Economic Forum. *Quantum Readiness Toolkit: Building a Quantum-Secure Economy*; Technical Report; World Economic Forum: Geneva, Switzerland, 2023. Available online: https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/ (accessed on 18 July 2025).
22. National Institute of Standards and Technology. *Considerations for Transitioning to Post-Quantum Cryptographic Algorithms*; Interagency report (ir) 8547 (initial public draft); U.S. Department of Commerce: Washington, DC, USA, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf (accessed on 5 July 2025).
23. Kumar, G. Quantum Risk Assessment: Understanding and Scoring Data Sensitivity and Exposure. *LinkedIn Pulse*, June 2025. Available online: https://www.linkedin.com/pulse/quantum-risk-assessment-understanding-scoring-data-sensitivity-n-pvzic/ (accessed on 3 July 2025).
24. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Off. J. Eur. Union* **2016**, *L119/1*, 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed on 18 July 2025).
25. Cox, A.; Richardson, M.; Graham, E.; Castro, H. Risk Assessment Frameworks for Post-Quantum Cryptographic Migration in Cloud Systems. *Preprint* **2025**. Available online: https://www.researchgate.net/publication/391913205 (accessed on 18 July 2025).
26. evolutionQ Inc. Quantum Risk Assessment Services. 2024. Available online: https://www.evolutionq.com/services/quantum-risk-assessment (accessed on 3 July 2025).
27. AvinyaSQ. Quantum Risk Assessment (QRA). 2024. Available online: https://avinyasq.com/quantum-risk-assessment-qra (accessed on 3 July 2025).
28. Mosca, M.; Mulholland, J. A Methodology for Quantum Risk Assessment. 2017. Available online: https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/ (accessed on 12 July 2025).
29. Kiviharju, M. Refining Mosca's Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security. In *Cyber Security: Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 369–401.
30. The White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). Presidential Memorandum. 2022. Available online: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed on 12 July 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.