Development and Preliminary Validation of PQC-ORI: A Public-Sector Readiness Assessment Instrument for Post-Quantum Cryptography

Fadlilah Izzatus Sabila[1*], Fauziah[2]

[1,2] *Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional, Jl. Sawo Manila No.61, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta, 12520, Indonesia*

E-mail: fadlilahizzatussabila.2024@student.unas.ac.id, fauziah@civitas.unas.ac.id

*Corresponding Author

Abstrak— **Perkembangan teknologi komputasi kuantum menimbulkan risiko signifikan terhadap sistem kriptografi kunci publik konvensional serta meningkatkan urgensi kesiapan organisasi dalam menghadapi migrasi menuju Post-Quantum Cryptography (PQC). Meskipun berbagai framework migrasi PQC dan inisiatif quantum-readiness telah dikembangkan, pendekatan yang ada umumnya masih berfokus pada panduan migrasi teknis dan belum menyediakan mekanisme operasional yang memadai untuk mengukur kesiapan organisasi, khususnya pada lingkungan sektor publik. Penelitian ini bertujuan untuk mengembangkan dan melakukan validasi awal *Post-Quantum Cryptography Organizational Readiness Instrument* bagi organisasi sektor publik di Indonesia. Penelitian menggunakan pendekatan Design Science Research dengan mengintegrasikan *Systematic Literature Review*, *Qualitative Content Analysis*, dan *Framework Alignment Matrix*. Hasil penelitian menghasilkan instrument penilaian kesiapan organisasi yang terdiri atas enam dimensi, yaitu *Cryptographic Awareness, Governance and Policy, Migration Management, Technical Capability, Cryptographic Agility*, dan *Operational Resilience* yang dioperasionalisasikan ke dalam indikator terstruktur dan model kematangan lima tingkat. Validasi awal oleh tiga pakar menggunakan *structured expert judgement* menghasilkan nilai rata-rata 3,69 dari 4,00 yang menunjukkan tingkat relevansi, konsistensi konseptual, dan keterterapan yang tinggi. Penelitian ini memberikan kontribusi berupa instrumen penilaian kesiapan organisasi yang dapat mendukung penilaian mandiri, perencanaan migrasi PQC, serta penelitian empiris lanjutan.**

***Kata Kunci* — *Post-Quantum Cryptography*; Model Kesiapan Organisasi; Instrumen Penilaian Kesiapan; *Design Science Research*; Sektor Publik.**

Abstract— **The emergence of quantum computing technologies poses significant risks to conventional public-key cryptographic systems and creating an urgent need for organizational preparation toward Post-Quantum Cryptography (PQC) migration. Although various PQC migration frameworks and quantum-readiness initiatives have been proposed, existing approaches primarily focus on technical migration guidance and provide limited operational mechanisms for assessing organizational readiness, particularly within public-sector environments. This study develops and conducts a preliminary validation of a Post-Quantum Cryptography Organizational Readiness Instrument (PQC-ORI) for Indonesian public-sector organizations using a Design Science Research approach integrating Systematic Literature Review (SLR), Qualitative Content Analysis (QCA), and Framework Alignment Matrix (FAM) techniques to synthesize recurring organizational readiness constructs from PQC migration literature, governance frameworks, and cybersecurity readiness studies. The resulting framework comprises six organizational readiness dimensions: Cryptographic Awareness, Governance and Policy, Migration Management, Technical Capability, Cryptographic Agility, and Operational Resilience. The framework additionally operationalizes these dimensions into structured assessment indicators and a five-level maturity model intended to support organizational self-assessment and migration planning activities. Preliminary validation by three domain experts using structured expert judgment yielded an overall mean score of 3.69/4.00, indicating high relevance, conceptual consistency, and applicability for assessing organizational readiness for PQC migration in public-sector organizations.**

Keywords* — Post-*Quantum Cryptography; Organizational Readiness Framework; Readiness Assessment Instrument; Design Science Research; Public Sector.

I. INTRODUCTION

The rapid advancement of quantum computing technologies is expected to fundamentally disrupt the security foundations of contemporary public-key cryptographic systems. Widely deployed cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) are considered vulnerable to future quantum-enabled attacks due to the computational capabilities introduced by Shor's algorithm [1]. As a consequence, encrypted data collected today may eventually be decrypted once sufficiently capable quantum computers become operational, creating a significant cybersecurity concern commonly referred to as "Harvest Now, Decrypt Later" (HNDL) or "Store Now, Decrypt Later" (SNDL) [2]. This threat is particularly critical for government organizations and public-sector institutions that manage sensitive information requiring long-term confidentiality, including citizen data, national strategic information, and critical digital infrastructure services.s

In response to these emerging risks, international organizations, standardization bodies, and national cybersecurity agencies have initiated various Post-Quantum Cryptography (PQC) migration frameworks and quantum-readiness guidelines, including ETSI, NIST, WEF, ENISA CSA Singapore, QRWG Canada, BSI Germany, ETDA Thailand, BSSN Indonesia, AIVD/CWI/TNO Netherlands, and CERT-In India, [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]. These initiatives generally emphasize migration planning, cryptographic inventory, interoperability management, hybrid deployment strategies, and crypto-agility mechanisms to support long-term quantum-safe transition.

Nevertheless, PQC migration extends beyond the technical replacement of cryptographic algorithms. The transition introduces broader organizational challenges associated with governance structures, migration coordination, operational continuity, workforce capability, vendor dependency, interoperability management, and long-term organizational adaptability. Consequently, PQC migration readiness represents a multidimensional socio-technical challenge involving governance, operational, and organizational transformation considerations.

Recent studies have begun addressing organizational aspects of quantum-safe transition. Kong et al. [13] proposed a socio-technical organizational readiness model for quantum-safe transition, while Hohm et al. [14] introduced a maturity-oriented approach for assessing cryptographic agility. Additional studies such as QUASAR [15], RMQuantum [16], QORL [17], and quantum cybersecurity maturity frameworks [18], [19], [20] have further expanded the discussion toward governance capability, organizational preparedness, and migration management. Table 1 summarizes several prominent PQC migration and readiness frameworks discussed in the literature.

Existing PQC migration frameworks predominantly prescribe what organizations should do during migration, including cryptographic discovery, algorithm transition, hybrid deployment, and governance planning. However, they provide limited support for systematically determining whether organizations possess the governance, technical, operational, and organizational capabilities required to initiate and sustain PQC migration. Furthermore, existing studies rarely operationalize organizational readiness into measurable constructs, assessment indicators, scoring mechanisms, and maturity criteria that comprehensively capture governance, cryptographic awareness, migration management, technical capability, crypto agility, and operational resilience. Consequently, readiness evaluation remains largely dependent on qualitative judgment rather than a structured and repeatable assessment process. As a result, organizations lack a standardized mechanism to identify readiness gaps, prioritize migration activities, and monitor readiness improvement over time.

This limitation is particularly relevant for public-sector organizations, especially in developing-country contexts where legacy infrastructure, regulatory obligations, resource constraints, and interdependent digital services complicate PQC migration. Indonesia provides a representative application context because its public-sector organizations operate within highly regulated environments characterized by legacy information systems, interdependent digital government services, and long-term protection requirements for sensitive information, all of which increase the complexity of PQC migration.

To address this gap, this study develops and preliminary validates the Post-Quantum Cryptography Organizational Readiness Instrument (PQC-ORI) for Indonesian public sector organizations. The study adopts Design Science Research Methodology (DSRM) [21], [22] to develop a socio-technical assessment artifact through the integration of Systematic Literature Review (SLR),

Qualitative Content Analysis (QCA) [23], [24], and Framework Alignment Matrix (FAM) [18]. QCA was selected to systematically extract recurring organizational readiness constructs from heterogeneous literature sources, while FAM was employed to evaluate conceptual alignment and reduce overlap among synthesized readiness domains. The proposed instrument operationalizes organizational readiness into structured dimensions, indicators, and a five-level maturity model that supports organizational self-assessment and migration planning.

This study makes three contributions to the PQC migration literature. First, it develops an operational organizational readiness assessment instrument that translates socio-technical readiness into measurable dimensions, indicators, and maturity levels. Second, it contextualizes PQC readiness assessment for Indonesian public-sector organizations. Third, it demonstrates how DSRM, SLR, QCA, and FAM can be integrated to support the systematic development of cybersecurity readiness assessment instruments.

Table 1. Comparison of existing PQC Readiness Frameworks

Framework	Primary Focus	Readiness Orientation	Limitation	Assessment Operationalization
ENISA (2021)	Quantum threat mitigation	Technical migration readiness	Limited organizational assessment	Primarily technical and migration-oriented
WEF (2023)	Governance readiness	Strategic organizational readiness	Limited operational indicators	Strategic-level governance recommendations
ETSI TR 103 619 (2023)	Migration lifecycle	Technical transition readiness	Limited maturity assessment	Technical migration lifecycle guidance
TNO Handbook (2024)	PQC migration management	Lifecycle-based readiness	More implementation-oriented	Operational migration and risk management guidance
Kong et al. (2024)	Organizational readiness for quantum-safe transition	Socio-technical organizational readiness	Limited operationalized assessment indicators	Conceptual socio-technical readiness model
CSA QRI (2025)	Organizational readiness	Capability assessment	Limited migration operationalization	Structured capability scoring mechanism
CAMM (2022)	Crypto-agility maturity	Maturity-based readiness	Narrow organizational scope	Specialized crypto-agility maturity assessment
QORL (2024)	Organizational readiness maturity	Progressive readiness levels	Limited technical depth	Organizational readiness maturity progression model
PQC-ORI (This Study)	Organizational PQC readiness	Socio-technical maturity-oriented assessment	Preliminary validation and limited empirical implementation	Operationalized socio-technical organizational readiness assessment instrument with structured indicators and maturity interpretation

II. RESEARCH METHODOLOGY

This study adopted DSRM to develop a PQC-ORI for the Indonesian public sector. DSRM was selected because the primary objective of the study was not merely to investigate a phenomenon, but to develop a structured assessment artifact capable of addressing a practical organizational problem related to PQC migration readiness. The methodology enables the systematic development of artifacts that are theoretically grounded while remaining applicable within real organizational contexts.

The research process consisted of six major stages: problem identification, literature synthesis, conceptual framework development, instrument operationalization, preliminary expert validation, and initial evaluation.

Research Design

This study aimed to develop a socio-technical assessment artifact capable of representing organizational preparedness for PQC migration in a structured and operationalized manner. The proposed artifact was designed to support organizational self-assessment processes, readiness gap identification, and preliminary migration preparedness evaluation within public-sector institutions.

The DSRM approach was considered appropriate because the study involved iterative artifact construction, conceptual refinement, and preliminary evaluation processes. Furthermore, DSRM has been widely adopted in information systems and cybersecurity research involving framework development, assessment model construction, and instrument design. The overall methodological workflow is illustrated in Figure 1. The workflow demonstrates the iterative nature of DSRM, in which outputs from each stage informed the subsequent artifact refinement and evaluation activities.

Literature Synthesis

An SLR was conducted to establish the conceptual foundation of the proposed PQC-ORI framework. The review aimed to identify recurring organizational readiness constructs, governance capabilities, migration practices, and socio-technical factors related to PQC transition. Literature sources were collected from Scopus, IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar, complemented by migration frameworks and technical guidance published by international standardization bodies and cybersecurity agencies. Literature published between 2020 and 2026 was prioritized to capture recent developments in PQC migration and quantum-readiness research.

The search process employed combinations of keywords including "post-quantum cryptography migration," "quantum readiness," "cryptographic agility," "organizational readiness," and "quantum-safe transition." The inclusion criteria prioritized studies discussing governance capability, migration management, interoperability, cryptographic agility, and operational aspects of PQC transition, while studies focused solely on cryptographic algorithm performance were excluded. Literature screening was conducted through title, abstract, and full-text evaluation to ensure relevance to the study objectives.

Figure 2 presents the literature identification and selection process using the PRISMA 2020 flow diagram [25]. PRISMA was employed solely as a reporting guideline to improve the transparency and reproducibility of the literature selection process conducted during the Systematic Literature Review phase of the DSRM. A total of 122 records were initially identified through database searches. Following title and abstract screening, 57 records were excluded, resulting in 65 reports retrieved for full-text assessment. After eligibility evaluation, 43 reports were excluded because they were not relevant to organizational readiness, focused exclusively on technical or algorithmic aspects of PQC, or did not address PQC migration or organizational readiness frameworks. Consequently, 22 studies satisfied the eligibility criteria and were included in the subsequent concept synthesis and FAM analysis.

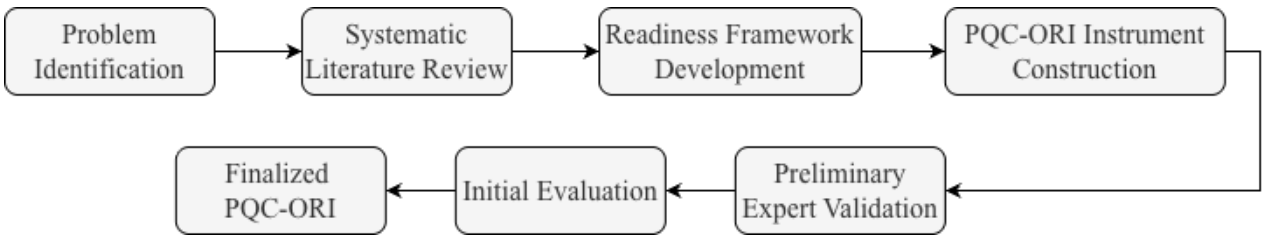

Figure 1. Research Workflow for The Development and Preliminary Validation of PQC-ORI using Design Science Research Methodology (DSRM).

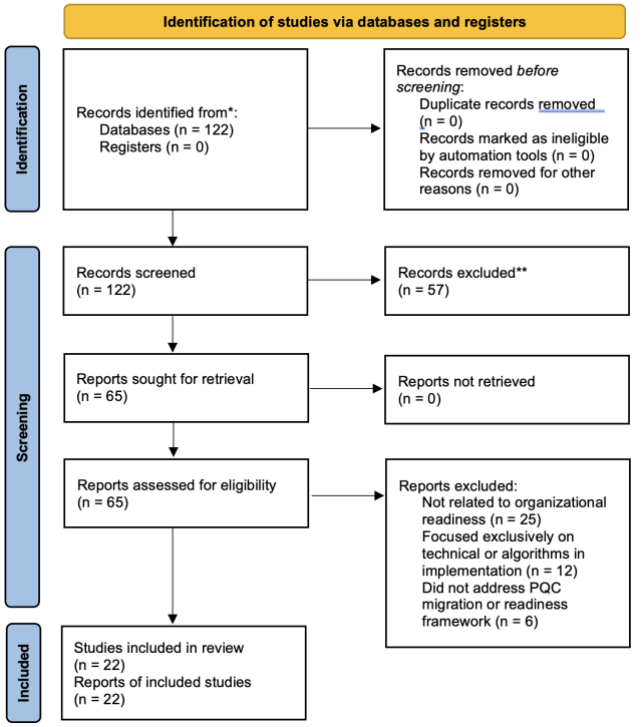

Figure 2. The PRISMA Diagram

The final literature corpus comprised 22 selected studies, including peer-reviewed publications as well as institutional frameworks, migration guidelines, technical handbooks, and policy documents. The inclusion of institutional and gray literature was considered appropriate because organizational guidance for PQC migration is currently driven not only by academic research but also by international standards organizations, cybersecurity agencies, and national migration initiatives.

Directed QCA was subsequently employed to extract recurring socio-technical readiness constructs from the selected literature. The coding process was conducted by the principal researcher using a predefined coding protocol derived from the research objectives and eligibility criteria. A single-coder approach was adopted because the purpose of the analysis was concept extraction to support artifact development rather than qualitative interpretation of participant-generated data. The unit of analysis included governance mechanisms, migration capability descriptions, cryptographic management practices, operational recommendations, and organizational readiness statements identified within the reviewed sources. Coding consistency was maintained through iterative refinement of the coding scheme, repeated comparison with the original literature, and cross-validation during the subsequent FAM synthesis.

To strengthen conceptual consistency and reduce construct overlap, this study additionally employed the FAM as a structured synthesis technique. Following concept extraction through Directed QCA, the identified organizational readiness constructs were systematically compared across the 22 selected frameworks.

Each readiness construct was examined to determine whether it was explicitly addressed, partially addressed, or not identified within each framework. The occurrence of these three levels of support was subsequently summarized for every readiness domain to improve the transparency of the synthesis process. Rather than applying a quantitative scoring model or predefined alignment categories, the FAM was interpreted qualitatively by examining the distribution of explicit, partial, and absent support across the reviewed literature.

The FAM analysis supported the refinement of the synthesized framework by identifying recurring organizational readiness constructs, minimizing conceptual overlap, consolidating similar concepts, and recognizing organizational capability areas that were consistently represented or comparatively underrepresented in the existing literature. The resulting synthesis process supported dimensional refinement, prioritization, and the development of the final PQC-ORI readiness structure.

Instrument Development

The instrument development stage operationalized the synthesized readiness dimensions into measurable organizational assessment indicators. The resulting instrument, referred to as PQC-ORI, was designed as a maturity-oriented readiness assessment instrument consisting of organizational dimensions, structured indicators, and readiness interpretation criteria. The synthesis and refinement process resulted in six organizational readiness dimensions: Cryptographic Awareness, Governance, Migration Management, Technical Capability, Cryptographic Agility, and Operational Resilience.

Each dimension was subsequently operationalized into structured indicators representing organizational capabilities associated with post-quantum transition readiness. The indicators were developed by considering recurring constructs identified in the literature, organizational applicability, public-sector contextual relevance, and conceptual consistency across dimensions.

The instrument adopted a five-level maturity-oriented readiness interpretation ranging from Initial to Adaptive readiness conditions consistent with capability maturity and progressive organizational readiness assessment approaches commonly adopted in cybersecurity governance and organizational capability models [18], [19]. Rather than functioning as a binary checklist, the maturity interpretation was intended to represent the progressive implementation capability of organizations in preparing and managing PQC migration processes. To improve contextual applicability, the indicators and readiness interpretations were additionally adjusted to reflect the characteristics of Indonesian public-sector organizations, including governance structures, interoperability constraints, legacy system dependency, and institutional resource limitations.

Figure 3 illustrates the artifact development process through which the synthesized organizational readiness dimensions were systematically transformed into operational assessment indicators and maturity-based readiness interpretation.

Preliminary Expert Validation

Preliminary validation of the proposed PQC-ORI framework was conducted through a staged expert-based evaluation involving academics, government representatives, and cybersecurity practitioners with expertise in cryptography, cybersecurity governance, and PQC-related transition initiatives. Experts were selected using purposive sampling based on professional experience and domain relevance. Table 2 shows the profile of the experts participated in the instrument validation process.

The initial validation stage involved three experts and focused on evaluating the relevance, clarity, consistency, and organizational applicability of the proposed readiness dimensions, indicators, and maturity interpretations. Two experts completed structured scoring and evaluation procedures, while one expert primarily contributed qualitative refinement feedback due to the exploratory nature of the framework. Feedback obtained during the evaluation process was subsequently used to refine indicator wording, improve dimensional consistency, and strengthen contextual applicability.

A second-stage evaluation using the revised framework was subsequently initiated to further assess organizational interpretability and applicability, with the evaluation process remaining ongoing at the time of this study. At this stage, the validation focused on preliminary content-level and conceptual assessment rather than formal statistical validation or large-scale empirical implementation testing.

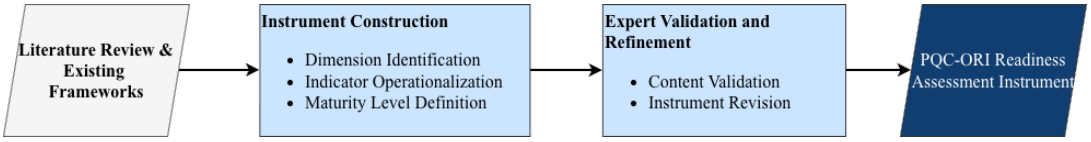

Figure 3. Development Process of the Proposed PQC-ORI Readiness Assessment Instrument

Table 2. The Expert Profile

Expert	Sector	Expertise	Experience
E1	Government	Cybersecurity governance	>20 years
E2	Academic	PQC research	>25 years
E3	Government	Cryptographic implementation	>10 years

Initial Evaluations

An initial evaluation stage was conducted to assess the practical applicability of the proposed instrument as a self-assessment mechanism for public-sector organizations. The evaluation focused on usability-related aspects, including clarity of readiness interpretation, organizational applicability, consistency of assessment logic, and feasibility of implementation within government organizational environments.

The evaluation at this stage did not aim to measure empirical effectiveness or predictive organizational outcomes. Instead, the objective was to ensure that the proposed instrument remained conceptually coherent and practically interpretable prior to future large-scale implementation and statistical validation studies.

III. RESULT AND DISCUSSION

Literature Synthesis Result

The synthesis demonstrates that recent discussions on PQC migration have evolved beyond purely technical cryptographic implementation toward broader organizational and governance-oriented readiness perspectives. Through the directed QCA, recurring concepts related to governance capability, cryptographic visibility, migration management, technical preparedness, cryptographic agility, operational resilience, workforce capability, and organizational risk management were identified and subsequently consolidated into higher-level organizational capability categories. These synthesized categories provided the conceptual foundation for developing the proposed PQC-ORI readiness framework. Table 3 summarizes the results of the QCA synthesis.

The synthesis demonstrated that recent PQC migration discussions have evolved beyond purely technical cryptographic implementation concerns toward broader organizational and governance-oriented readiness perspectives.

Table 4 summarizes the distribution of organizational readiness domains identified through the FAM. The results indicate that Sustainability and Continuity Readiness received the highest level of explicit support, appearing in 21 of the 22 reviewed frameworks (95.5%). This was followed by Transition and Migration Management and Maturity and Continuous Improvement, each explicitly represented in 19 frameworks (86.4%), while Risk and Impact Management appeared explicitly in 18 frameworks (81.8%). Similarly, Governance and Strategic Management and Operational and Process Capability were explicitly supported by 17 frameworks (77.3%), indicating broad agreement regarding their importance for organizational readiness toward PQC migration.

In contrast, several domains demonstrated lower levels of explicit representation while still appearing as partially addressed concepts across numerous frameworks. Innovation and Research Capability received explicit support from only five frameworks (22.7%), although it appeared as a partially addressed construct in 16 additional frameworks, suggesting that innovation is increasingly recognized but has not yet been comprehensively operationalized within current PQC migration guidance. Likewise, Resource and Investment Management was explicitly addressed by nine frameworks (40.9%), with 10 frameworks discussing the topic only partially, indicating that long-term investment planning and resource allocation remain comparatively less developed within existing organizational readiness frameworks.

Overall, the FAM synthesis demonstrates a clear evolution in the PQC migration literature. Earlier studies predominantly emphasized cryptographic algorithms, standards, and migration techniques, whereas more recent frameworks increasingly conceptualize organizational readiness as a multidimensional capability encompassing governance, cryptographic visibility, migration management, technical capability, operational resilience, and continuous improvement. This trend reinforces the need for a comprehensive organizational readiness framework capable of integrating these interrelated capabilities into a unified readiness assessment model, which forms the conceptual foundation of the proposed PQC-ORI framework.

Table 3. QCA-Based Organizational Readiness Synthesis Results

Axial Category	Representative Constructs	Supporting Literature	Contribution to PQC-ORI Development
Governance and Strategic Management	Governance readiness, strategic coordination	WEF, Kong et al., BSSN	Supported governance indicators
Cryptographic Visibility	Cryptographic inventory, dependency visibility	ENISA, TNO, ETSI TR 104 016	Supported awareness indicators
Cryptographic Agility and Interoperability	Algorithm flexibility, interoperability	CAMM, BSI, CSA Handbook	Supported agility indicators
Transition and Migration Management	Migration planning, phased transition	ETSI TR 103 619, PQCC	Supported migration indicators
Technical and Infrastructure Capability	Infrastructure readiness, integration capability	QUASAR, RMQuantum	Supported technical capability indicators
Operational and Process Capability	Operational coordination, implementation capability	QUASAR, CSA QRI	Supported operational capability indicators
Risk and Impact Management	Risk assessment, vulnerability awareness	ENISA, CERT-In	Supported risk assessment indicators
Workforce and Organizational Capability	Workforce readiness, awareness development	ETDA Thailand, WEF	Supported workforce capability indicators
Ecosystem and Stakeholder Collaboration	Stakeholder coordination, dependency management	WEF, NIST IR 8547	Supported collaboration indicators
Compliance, Assurance and Regulatory Capability	Regulatory governance, assurance capability	BSSN, CSA Handbook	Supported compliance indicators
Resource and Investment Management	Resource allocation, investment readiness	QUASAR, Malaysia Framework	Supported resource readiness indicators
Maturity and Continuous Improvement	Continuous improvement, adaptive capability	QORL, RMQuantum	Supported maturity interpretation
Sustainability and Continuity Readiness	Operational continuity, resilience capability	QUASAR, CERT-In	Supported resilience indicators
Innovation and Research Capability	Innovation readiness, technology adaptation	RMQuantum, WEF	Supported adaptability considerations

Table 4. Summary of Organizational Readiness Domain Occurrence Across Selected PQC Frameworks

FAM Domain	Explicit	Partial	Not Identified	Explicit Support (%)
Governance and Strategic Management	17	5	0	77.3%
Cryptographic Visibility	14	7	1	63.6%
Cryptographic Agility and Interoperability	16	6	0	72.7%
Transition and Migration Management	19	3	0	86.4%
Technical and Infrastructure Capability	16	6	0	72.7%
Operational and Process Capability	17	5	0	77.3%
Risk and Impact Management	18	4	0	81.8%
Workforce and Organizational Capability	15	7	0	68.2%
Ecosystem and Stakeholder Collaboration	12	8	2	54.5%
Compliance, Assurance and Regulatory Capability	14	7	1	63.6%
Resource and Investment Management	9	10	3	40.9%
Maturity and Continuous Improvement	19	3	0	86.4%
Sustainability and Continuity Readiness	21	1	0	95.5%
Innovation and Research Capability	5	16	1	22.7%

Organizational Readiness Dimensions Development and Analysis

The selective coding and conceptual refinement process resulted in six organizational readiness dimensions representing the socio-technical capability required to support PQC migration within public-sector organizations. Table 5 shows final readiness dimensions for the proposed PQC-ORI framework. The resulting dimensions were developed through iterative synthesis, overlap reduction, conceptual consolidation, and contextual refinement processes. The resulting synthesis is represented as the

conceptual structure of the proposed PQC-ORI framework, illustrating the relationship between the six readiness dimensions and their operationalization into assessment indicators, as shown in Figure 4.

As illustrated in Figure 4, the proposed PQC-ORI framework consists of six interrelated organizational readiness dimensions that collectively represent organizational preparedness for PQC migration. Rather than functioning as independent capability areas, the dimensions are operationalized through structured assessment indicators that enable systematic readiness evaluation using a maturity-based interpretation model.

The resulting dimensions demonstrate that organizational PQC readiness extends beyond technical implementation considerations toward broader governance, operational, and institutional preparedness capabilities. Cryptographic Awareness emerged as a foundational readiness capability because organizational visibility of cryptographic assets and dependency exposure strongly influences migration prioritization, risk identification, and transition planning processes. This finding aligns with governance-oriented readiness frameworks emphasizing the importance of cryptographic visibility and organizational awareness during quantum-safe transition initiatives [8], [10], [12], [15], [26]. Within governmental and public digital service environments, awareness-related challenges may become more significant due to varying institutional maturity levels, limited PQC familiarity, and dependency on legacy digital infrastructures.

The synthesis results consistently positioned Governance and Policy capability as a dominant readiness dimension because PQC migration requires long-term organizational coordination, strategic decision-making, policy alignment, and resource prioritization beyond purely technical implementation activities. The reviewed frameworks consistently emphasized governance readiness as a critical factor for supporting migration planning, institutional accountability, and cross-functional coordination during quantum-safe transition processes. This observation is consistent with governance-oriented readiness approaches proposed by WEF [5], CSA QRI [6], and Kong et al. [13], which highlight the importance of institutional leadership and organizational coordination mechanisms in managing large-scale cryptographic transformation initiatives. In public-sector organizations, governance-related readiness becomes increasingly important due to regulatory obligations, procurement dependency, hierarchical decision structures, and cross-agency interoperability requirements.

Migration-related capability was identified as a critical organizational readiness requirement due to PQC transition is expected to occur gradually through phased implementation, hybrid cryptographic deployment, and long-term migration coordination processes. The literature synthesis indicates that organizations require structured migration planning capabilities to prioritize cryptographic replacement activities, manage interoperability constraints, and minimize operational disruption during transition phases. This finding is strongly reflected in migration-oriented frameworks such as ETSI TR 103 619 [3], BSSN [8], and the TNO migration handbook [10], which emphasize staged migration approaches and cryptographic lifecycle management. In institutional environments with interconnected digital services and multi-vendor ecosystems, migration coordination challenges may become more complex due to legacy infrastructure dependency and interoperability requirements.

Technical Capability additionally emerged as a core readiness dimension due to the operational complexity associated with identifying, evaluating, and replacing vulnerable cryptographic dependencies across organizational infrastructures.

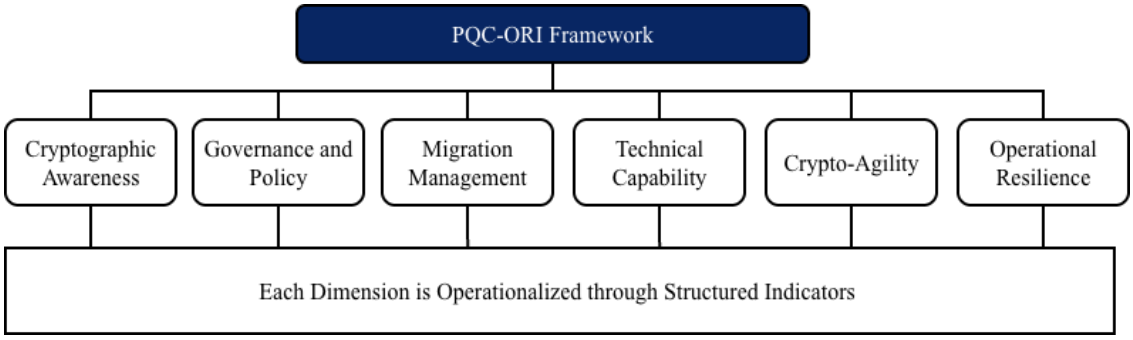

Figure 4. Conceptual Structure of the Proposed PQC-ORI Organizational Readiness Framework

The synthesis results demonstrate that interoperability management, cryptographic inventory visibility, asset discovery, and infrastructure compatibility represent recurring concerns across PQC migration literature. Existing migration frameworks consistently emphasize the importance of technical preparedness for maintaining service continuity during cryptographic transition processes [3], [27]. Within government-sector digital infrastructures, technical readiness challenges may be amplified by heterogeneous infrastructure conditions, procurement limitations, and long system replacement cycles.

Crypto Agility emerged as a strategically important readiness dimension because PQC migration is expected to remain an evolving and iterative process rather than a one-time cryptographic replacement activity. The uncertainty surrounding future cryptographic standardization, algorithm maturity, and interoperability requirements necessitates organizational capability to adapt cryptographic mechanisms continuously over time. This finding aligns with previous crypto-agility and migration readiness studies emphasizing adaptability, modular cryptographic architecture, and rapid algorithm transition capability as essential components of long-term quantum resilience [13], [14], [26]. For public-sector organizations, crypto-agility additionally supports long-term policy adaptability and reduces dependency on rigid infrastructure replacement cycles.

Operational Resilience emerged as a supporting readiness dimension because PQC migration may introduce service disruption risks, interoperability instability, and transitional operational uncertainty during cryptographic replacement processes. The literature synthesis suggests that organizations must maintain continuity of critical digital services while simultaneously implementing cryptographic transformation initiatives [6], [15], [28]. This consideration becomes particularly important within public-sector organizations responsible for delivering essential public services and managing critical digital infrastructures. The emergence of this dimension further reinforces the view that PQC migration should be treated as a long-term organizational transformation process rather than a purely technical implementation activity.

Overall, the resulting dimensions demonstrate that organizational PQC readiness should be interpreted as a multidimensional institutional capability rather than a purely technical migration concern. The synthesis findings indicate that successful PQC transition depends not only on cryptographic implementation readiness, but also on governance coordination, organizational adaptability, migration planning capability, and long-term operational sustainability. Compared with several existing frameworks that primarily emphasize technical migration guidance, the proposed PQC-ORI framework integrates governance, technical, operational, and organizational readiness considerations into a unified socio-technical assessment structure applicable to public-sector environments.

Table 5. Final Readiness Dimensions

Dimension	Primary Focus	Definition
Cryptographic Awareness	Cryptographic visibility and risk awareness	Represents the organization's capability to identify, understand, and evaluate cryptographic assets, dependencies, and quantum-related exposure.
Governance and Policy	Strategic and organizational coordination	Represents the organizational structures, governance mechanisms, policies, and strategic coordination required to support PQC migration initiatives.
Migration Management	Transition planning and migration coordination	Represents the organizational capability to coordinate, manage, and monitor phased PQC transition and migration activities.
Technical Capability	Technical implementation and infrastructure readiness	Represents the technical capability required to implement, integrate, validate, and operationalize PQC technologies and supporting infrastructure.
Cryptographic Agility	Interoperability and adaptive cryptographic transition	Represents the organizational capability to maintain cryptographic flexibility, interoperability, and adaptive transition mechanisms during PQC migration.
Operational Resilience	Continuity, adaptability, and long-term sustainability	Represents the organizational capability to sustain operational continuity, organizational adaptability, and long-term resilience throughout PQC migration processes.

Instrument Operationalization

Following the dimension development process, the study operationalized each readiness dimension into structured organizational assessment indicators. The operationalization process aimed to transform recurring conceptual constructs into measurable readiness capabilities applicable within organizational assessment processes. Indicator development and refinement were conducted iteratively by considering construct recurrence across the literature, conceptual representativeness, organizational applicability, dimensional distinctiveness, and public-sector contextual relevance. Indicators demonstrating excessive conceptual overlap or limited organizational interpretability were refined, consolidated, or removed during the development process to improve assessment clarity and dimensional consistency across the proposed framework.

The operationalization process additionally considered the feasibility of organizational self-assessment implementation to ensure that the resulting indicators remained interpretable and applicable within heterogeneous public-sector organizational environments. Rather than functioning as technical implementation checklists, the indicators were designed to represent organizational capabilities associated with preparing, governing, implementing, and sustaining the transition toward Post-Quantum Cryptography. Contextual adaptations were also introduced to reflect characteristics of Indonesian public-sector organizations, including governance complexity, interoperability requirements, legacy system dependencies, vendor coordination, and institutional resource constraints. These adaptations were considered necessary because most existing PQC migration frameworks were developed within organizational contexts characterized by different governance structures, regulatory environments, and cybersecurity maturity levels.

To enable systematic organizational assessment, each indicator is evaluated using a five-point readiness scale that reflects the organization's current capability. Consistent with the Equal Capability Assessment Approach adopted in this study, all indicators are treated as having equal conceptual contribution because each indicator represents an essential organizational readiness capability synthesized through the SLR, Directed QCA, and FAM. The readiness score for each organizational dimension is calculated as the arithmetic mean of the indicator scores within that dimension, as expressed in Equation (1), where D_i denotes the readiness score of dimensions i, I_{ij} represents the score assigned to indicator j within dimension i, and n is the number of indicators in dimension.

$$D_i = \frac{\sum_{j=1}^{n} I_{ij}}{n} \qquad (1)$$

The overall organizational readiness score (PQC-ORI) is subsequently calculated as the arithmetic mean of the readiness scores across all organizational dimensions, as presented in Equation (2), where $PQC\text{-}ORI$ denotes the overall organizational readiness score, D_i represents the readiness score of dimensions i, and m is the total number of readiness dimensions included in the assessment framework.

$$\text{PQC} - \text{ORI} = \frac{\sum_{i=1}^{m} D_i}{m} \qquad (2)$$

Table 6 presents the operationalized indicators and their corresponding assessment parameters used to evaluate organizational readiness across the proposed PQC-ORI dimensions. The assessment therefore produces dimension-level readiness scores and a composite organizational readiness score that is subsequently interpreted using the maturity model presented in Table 7.

Table 6. Indicator Operationalization of the Proposed PQC-ORI Framework

Dimension	Indicator	Assessment Parameters
Cryptographic Awareness	Cryptographic asset inventory and visibility	Availability of documented inventory, asset visibility process, CBOM identification
	Dependency identification	Dependency mapping process, interoperability visibility, system dependency documentation
	Quantum threat awareness	Awareness of quantum threats, vulnerability understanding, exposure assessment
	Quantum risk assessment	Risk assessment procedure, prioritization mechanism, impact evaluation
	Migration impact awareness	Awareness of migration effort, transition complexity, operational impact
Governance and Policy	Governance framework	Governance policy, organizational structure, migration governance mechanism
	Policy and compliance mechanism	Compliance procedure, policy enforcement, regulatory alignment
	Stakeholder coordination	Stakeholder involvement, vendor coordination, ecosystem collaboration
	Resource and funding support	Budget allocation, investment planning, resource management
	Leadership commitment	Executive commitment, management engagement, policy support
Migration Management	Migration roadmap	Migration planning, roadmap documentation, transition sequencing
	Transition governance	Strategic migration planning, transition coordination, governance process
	Phased migration capability	Migration phases, staged implementation, execution capability
	Hybrid transition implementation	Hybrid cryptography usage, interoperability transition, hybrid deployment
	Migration monitoring and evaluation	Monitoring mechanism, readiness measurement, implementation evaluation
Technical Capability	Infrastructure readiness	Infrastructure preparedness, security architecture readiness, technical support capability
	PQC implementation capability	Deployment readiness, implementation capability, operational support
	System integration capability	Integration capability, interoperability integration, deployment integration
	Compatibility validation	Compatibility testing, algorithm validation, implementation assurance
	Research and testing capability	Pilot implementation, technology experimentation, validation activities
Cryptographic Agility	Interoperability capability	Interoperability resilience, extensibility, transition compatibility
	Legacy compatibility	Backward compatibility, legacy system support, transition continuity
	Algorithm flexibility	Algorithm adaptability, crypto-agility, flexibility mechanism
	Cryptographic replaceability	Replaceability, updateability, removability
	Adaptive cryptographic architecture	Adaptive architecture, long-term transition support, extensible cryptographic structure
Operational Resilience	Business continuity capability	Continuity readiness, service sustainability, operational resilience
	Risk monitoring capability	Risk monitoring, implementation risk management, mitigation process
	Workforce readiness	Workforce capability, staffing readiness, awareness development
	Continuous improvement capability	Readiness enhancement, maturity progression, capability improvement
	Sector adaptation capability	Contextual implementation, ecosystem alignment, sector adaptation

Maturity-Based Readiness Interpretation

To support assessment interpretability, the proposed instrument adopted a maturity-oriented readiness model using a five-level readiness scale ranging from Initial to Adaptive readiness conditions.

The maturity interpretation was designed to represent the progressive implementation capability of organizations rather than binary readiness states. The maturity structure allows organizations to evaluate readiness conditions across multiple dimensions while recognizing that organizational capability may evolve gradually over time. Accordingly, readiness assessment within the proposed framework does not solely measure the existence of organizational capability, but also evaluates implementation consistency, governance integration, operational sustainability, and organizational adaptability.

Unlike purely technical compliance-oriented assessments, the proposed maturity model emphasizes organizational preparedness and migration capability progression. This approach was selected because PQC migration is expected to occur incrementally through long-term organizational transition processes involving governance, interoperability management, operational continuity, and technological adaptation. The readiness interpretation was additionally designed to support practical organizational self-assessment processes by improving interpretability and reducing ambiguity during assessment activities. Table 7 presents the maturity readiness interpretation model.

Preliminary Expert Validation

Preliminary validation of the proposed PQC-ORI framework was conducted through expert evaluation involving academics, cybersecurity practitioners, and government-related experts with experience in PQC migration, cybersecurity governance, and cryptographic implementation. The evaluation assessed the relevance, clarity, conceptual consistency, applicability, and representativeness of the proposed readiness dimensions, indicators, and maturity interpretations within public-sector organizational contexts. The validation process was conducted iteratively through two stages. The initial stage focused on conceptual assessment and framework refinement through structured evaluation and qualitative feedback. The revised framework was subsequently reviewed through a second-stage evaluation to further assess dimensional interpretability, contextual applicability, and conceptual consistency.

Table 7. Maturity Readiness Interpretation

Level	Readiness Stage	Characteristics	PQC Readiness Interpretation
Level 1	Initial	Reactive and fragmented readiness	The organization demonstrates limited awareness of quantum-related threats and lacks formal governance, cryptographic visibility, migration planning, and PQC implementation mechanisms.
Level 2	Developing	Emerging but inconsistent readiness	The organization has initiated preliminary PQC readiness activities, including awareness development, cryptographic inventory, and initial migration planning, although implementation remains partial and insufficiently integrated across organizational processes.
Level 3	Defined	Documented and structured readiness	The organization has established documented governance structures, migration roadmaps, technical preparation mechanisms, and cryptographic management processes supporting PQC transition initiatives.
Level 4	Managed	Coordinated and measurable readiness	The organization actively manages PQC migration through coordinated governance, implementation monitoring, interoperability management, risk assessment, and organization-wide readiness evaluation mechanisms.
Level 5	Adaptive	Continuously adaptive readiness	The organization demonstrates mature and adaptive PQC readiness through continuous improvement, cryptographic agility, proactive transition optimization, ecosystem coordination, and long-term operational resilience.

The expert evaluation produced an overall mean score of 3.69 out of 4.00, indicating strong expert agreement regarding the conceptual adequacy and applicability of the proposed PQC-ORI framework. Among the evaluated components, the instrument structure obtained the highest evaluation (mean = 3.81), followed by the assessment model (mean = 3.73), while the readiness dimensions received a mean score of 3.52. Overall, these findings suggest that the proposed artifact demonstrates satisfactory content representation and conceptual consistency for preliminary organizational readiness assessment.

The qualitative feedback complemented the quantitative evaluation by identifying several areas requiring refinement. Experts observed that some indicators remained relatively technical for non-specialized respondents, particularly those addressing interoperability management, hybrid migration mechanisms, and cryptographic implementation activities. In addition, partial conceptual overlap was identified between the Migration Management and Technical Capability dimensions, suggesting that organizational readiness for PQC migration should be understood as an integrated socio-technical capability rather than a collection of isolated organizational functions.

Experts also highlighted several practical challenges that may influence future PQC migration within Indonesian public-sector organizations, including limited organizational awareness of quantum-related threats, workforce competency constraints, interoperability complexity, and continued dependence on legacy digital infrastructures. These observations reinforce the importance of governance preparedness, institutional coordination, organizational adaptability, and long-term migration planning as key enablers of sustainable quantum-safe transition

The expert feedback obtained during both validation stages was subsequently incorporated to refine indicator wording, improve dimensional consistency, reduce conceptual overlap, and strengthen contextual applicability. Accordingly, the reported findings should be interpreted as preliminary expert-based content validation supporting the conceptual feasibility of the proposed PQC-ORI framework. Broader empirical validation involving multiple public-sector organizations remains necessary to further evaluate the instrument's reliability, construct validity, and practical applicability.

Table 8. Preliminary Expert Validation Result

Evaluation Component	Mean Score
Instrument Structure	3.81
Readiness Dimensions	3.52
Assessment Model	3.73
Overall Mean	3.69

Table 9. Expert Validation Criteria for Preliminary PQC-ORI Validation

Evaluation Aspect	Evaluation Focus	Representative Evaluation Criteria	Relevance to Validation
Relevance	Conceptual suitability of dimensions and indicators	Indicators appropriately represent organizational PQC readiness constructs	Supports content validity assessment
Clarity	Wording clarity and interpretability	Indicator statements are clear and understandable	Supports consistency of expert evaluation
Consistency	Conceptual coherence across dimensions and indicators	Indicators are conceptually aligned with assigned dimensions	Supports construct coherence evaluation
Completeness	Coverage of organizational readiness domains	The framework sufficiently covers PQC readiness capability areas	Supports comprehensiveness assessment
Applicability	Practical feasibility within organizational environments	Indicators are applicable within public-sector organizational contexts	Supports practical usability evaluation
Concept Representation	Accuracy of construct representation	Indicators appropriately reflect intended readiness concepts	Supports conceptual validity evaluation

Discussion and Research Implications

The findings of this study suggest that organizational readiness for PQC migration should not be interpreted solely as a technical cryptographic replacement issue. Instead, PQC migration represents a long-term socio-technical organizational transformation process involving governance coordination, migration planning, interoperability management, institutional adaptation, and operational continuity. This observation reflects the growing shift within recent quantum-readiness discourse from purely technical migration considerations toward broader organizational and governance-oriented preparedness perspectives.

The synthesis process demonstrated that organizational readiness for PQC migration emerges from the interaction between governance capability, technical preparedness, migration coordination, cryptographic agility, and operational resilience. The resulting framework not only positions PQC readiness as a multidimensional organizational capability rather than an isolated cybersecurity implementation activity, but also translates this capability into a structured readiness assessment instrument that can be systematically applied within organizational settings. This finding is particularly important because many existing PQC migration initiatives continue to emphasize technical migration guidance without sufficiently operationalizing organizational readiness assessment mechanisms capable of supporting institutional preparedness evaluation [5], [13], [15].

The prominence of governance-related dimensions throughout the synthesis and validation stages additionally indicates that successful PQC migration may depend heavily on institutional coordination and strategic management capability. In large public-sector environments, migration activities are likely to involve complex decision structures, procurement dependency, regulatory obligations, vendor coordination, and interoperability challenges across interconnected digital services. Under such conditions, governance capability functions not only as an administrative mechanism, but also as an organizational enabler supporting migration prioritization, resource allocation, policy alignment, and long-term implementation sustainability.

The findings further highlight the strategic importance of cryptographic agility within long-term quantum-safe transition processes. Rather than representing a purely technical architectural feature, cryptographic agility may also be interpreted as an organizational adaptive capability that enables institutions to respond to evolving cryptographic standards [14], [29], interoperability requirements, implementation uncertainty, and future migration adjustments. This observation reinforces the growing recognition that quantum-safe transition is unlikely to occur through a single-stage migration process, but instead through continuous organizational adaptation over extended operational timelines.

From a public-sector perspective, the proposed framework also reflects organizational characteristics commonly associated with government digital environments, including legacy infrastructure dependency, heterogeneous system architectures, hierarchical governance structures, and cross-agency interoperability requirements. These conditions may significantly increase migration complexity and reduce organizational flexibility during long-term cryptographic transition initiatives. Consequently, readiness assessment within public-sector organizations requires broader evaluation dimensions extending beyond technical implementation readiness alone.

Methodologically, the study demonstrates the applicability of combining DSRM, directed QCA, and FAM approaches for developing organizational readiness assessment artifacts in emerging cybersecurity governance domains. The iterative synthesis and refinement process additionally illustrates how heterogeneous migration guidance, institutional frameworks, governance recommendations, and organizational readiness concepts can be consolidated into a structured socio-technical assessment framework.

Practically, unlike existing PQC migration guidance that primarily focuses on technical transition strategies, the proposed PQC-ORI operationalizes organizational readiness into a measurable assessment instrument that enables systematic readiness evaluation across governance, technical capability, migration management, cryptographic agility, and operational resilience. As such, the framework may support policymakers, regulators, and public-sector organizations in identifying organizational readiness conditions, prioritizing capability development, benchmarking institutional preparedness, and planning long-term quantum-safe transition initiatives. The framework may also provide an initial foundation for future readiness mapping activities and governance-oriented migration planning within Indonesian public-sector digital ecosystems.

Despite these contributions, the study remains subject to several limitations. The proposed framework has undergone preliminary expert-based conceptual evaluation but has not yet been empirically implemented across broader organizational environments. In addition, the limited number of domain experts involved in the validation process reflects the emerging and highly specialized nature of PQC migration expertise. Accordingly, the current findings should be interpreted as preliminary conceptual and content-level validation results rather than evidence of statistical construct validity or organizational performance effectiveness.

Future studies may extend the proposed framework through large-scale empirical implementation, psychometric validation, comparative inter-organizational assessment, and longitudinal readiness evaluation across multiple institutional sectors. Further refinement may also support sector-specific adaptation and integration with broader cybersecurity governance and digital transformation assessment initiatives.

IV. CONCLUSION

This study developed and conducted a preliminary validation of the Post-Quantum Cryptography Organizational Readiness Instrument (PQC-ORI) for Indonesian public-sector organizations. Using a Design Science Research approach combined with directed QCA- and FAM-based synthesis, the study produced a socio-technical organizational readiness assessment framework consisting of six readiness dimensions, structured organizational indicators, and maturity-based readiness interpretations intended to support PQC migration preparedness evaluation.

The proposed PQC-ORI provides a structured mechanism for assessing organizational readiness toward PQC migration by integrating organizational governance, technical capability, migration management, cryptographic agility, operational resilience, and cryptographic awareness into a unified readiness assessment framework. Unlike existing guidance documents, the instrument translates these readiness concepts into measurable indicators and maturity levels that can support evidence-based organizational assessment. Although preliminary expert validation indicates satisfactory content validity, broader empirical validation involving multiple public-sector organizations is required to evaluate construct validity, reliability, and practical applicability across different organizational contexts. Future studies may also investigate weighting strategies, benchmarking approaches, and longitudinal readiness assessment to support national quantum-safe migration initiatives.

Accordingly, PQC-ORI establishes an initial foundation for standardized organizational readiness assessment that may support strategic planning and policy development for post-quantum cryptography migration within the Indonesian public sector.

REFERENCES

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, pp. 124–134, 1994, doi: 10.1109/SFCS.1994.365700.

[2] M. Mosca and M. Piani, “Quantum Threat Timeline Report 2024,” 2024. Accessed: Nov. 28, 2025. [Online]. Available: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[3] ETSI, “Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies ,” Valbonne, Feb. 2025.

[4] NIST, “Quantum-Readiness: Migration to Post-Quantum Cryptography,” USA, Aug. 2023. Accessed: Nov. 28, 2025. [Online]. Available: https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF

[5] World Economic Forum and Deloitte, “Quantum Readiness Toolkit: Building a Quantum-Secure Economy,” Jun. 2023.

[6] CSA, “Quantum-Safe Handbook and Quantum Readiness Index | Cyber Security Agency of Singapore,” 2025. Accessed: Nov. 28, 2025. [Online]. Available: https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/

[7] QRWG of CFDIR, “Canadian National Quantum-Readiness,” Canada, Jul. 2024.
[8] BSSN, “Panduan Migrasi Ke Post-Quantum Cryptography Versi 1.0,” Bogorm West Java, Jan. 2026.
[9] ETDA, “PQC Migration Handbook for Thai Organizations,” 2026, [Online]. Available: https://qtft.github.io/pq-readiness-handbook/
[10] AIVD, CWI, and TNO, “The PQC Migration Handbook Guidelines for MIgrating to Post-Quantum Cryptography,” Dec. 2024.
[11] CERT-In and SISA, “Transitioning to Quantum Cyber Readiness.”
[12] Ward. Beullens *et al.*, *Post-quantum Cryptography : Current State and Quantum Mitigation*. [Publications Office of the European Union], 2021.
[13] I. Kong, M. Janssen, and N. Bharosa, “Navigating Through the Unknowns-Organizational Readiness Assessment Model for Quantum-Safe Transition,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Science and Business Media Deutschland GmbH, 2024, pp. 438–453. doi: 10.1007/978-3-031-70274-7_27.
[14] J. Hohm, A. Heinemann, and A. Wiesmaier, “Towards a Maturity Model for Crypto-Agility Assessment,” in *Foundations and Practice of Security*, L. and A. C. and S. F. and G.-A. J. Jourdan Guy-Vincent and Mounier, Ed., Cham: Springer Nature Switzerland, 2023, pp. 104–119.
[15] A. I. Weinberg, “Preparing for the Post Quantum Era: Quantum Ready Architecture for Security and Risk Management (QUASAR) - A Strategic Framework for Cybersecurity,” May 2025, [Online]. Available: http://arxiv.org/abs/2505.17034
[16] B. H. H. Al-Dulaimi, “TQSDRM: Towards Quantum Software Development Readiness Model (RMQuantum),” 2024.
[17] M. Teitsma, I. Ahmed, and J. van Velzen, “Quantum Organisational Readiness Levels,” Feb. 2025, Accessed: Nov. 26, 2025. [Online]. Available: https://arxiv.org/pdf/2502.16489
[18] T. Hardiana and S. Suhardi, “Design of a Cybersecurity Maturity Measurement Instrument for the Government Sector,” *Jurnal Pendidikan dan Teknologi Indonesia*, vol. 5, no. 11, pp. 3393–3310, Nov. 2025, doi: 10.52436/1.jpti.1124.
[19] US Department of Energy, “Cybersecurity Capability Maturity Model (C2M2),” Jun. 2022.
[20] Š. Grigaliūnas and R. Brūzgienė, “Towards a Unified Quantum Risk Assessment,” *Electronics 2025, Vol. 14, Page 3338*, vol. 14, no. 17, p. 3338, Aug. 2025, doi: 10.3390/ELECTRONICS14173338.
[21] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research 1,” *Design Science in IS Research MIS Quarterly*, vol. 28, no. 1, p. 75, 2004.
[22] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302;PAGE:STRING:ARTICLE/CHAPTER.
[23] H. F. Hsieh and S. E. Shannon, “Three approaches to qualitative content analysis,” *Qual. Health Res.*, vol. 15, no. 9, pp. 1277–1288, Nov. 2005, doi: 10.1177/1049732305276687.
[24] J. M. Corbin and A. Strauss, “Grounded theory research: Procedures, canons, and evaluative criteria,” *Qual. Sociol.*, vol. 13, no. 1, pp. 3–21, Mar. 1990, doi: 10.1007/BF00988593.
[25] “PRISMA 2020 flow diagram — PRISMA statement.” Accessed: Jul. 19, 2026. [Online]. Available: https://www.prisma-statement.org/prisma-2020-flow-diagram
[26] V. Erol, “Quantum Readiness in Cryptography: A Maturity-Based Framework for Post-Quantum Transition,” Oct. 02, 2025. doi: 10.20944/preprints202509.2584.v1.
[27] NIST, “Transition to Post-Quantum Cryptography Standards,” 2024, doi: 10.6028/NIST.IR.8547.IPD.
[28] ETSI, “TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes,” Jul. 2020.
[29] CSA, “(Draft for Public Consultation) Quantum-Safe Handbook,” Singapore, Oct. 2025.