IT SECTOR

Assessing Organisational Readiness for Post-Quantum Cryptography Migration in India's IT Sector: Indian IT Firms as Enterprises and as Migration Intermediaries

Manish Kumar Pandey, Kushagra Kartikey, Vaibhav Navle, Abhigyan Shukla

University of Economics – Varna, Varna, Bulgaria

Published November 2026

Abstract

Migration towards post-quantum cryptography (PQC) is now on the organizational agenda due to the standardization of three PQC algorithms by the U.S. National Institute of Standards and Technology in August 2024. However, while Indian information technology (IT) companies need to secure themselves as well as help their clients to migrate from cryptography vulnerable to quantum computing, empirical data regarding the PQC readiness of the aforementioned companies does not exist, and there is no existing validated measure of PQC readiness at firm level.

The current study seeks to devise and validate the Post-Quantum Cryptography Organisational Readiness Index (PORI), building on organisational readiness theory and Technology-Organization-Environment paradigm. Using exploratory sequential mixed methods research design, the project begins with conducting 12–15 interviews with security and technology executives exploring the state of readiness and the intermediary function played by IT service providers. Based on interviews' results, literature review, expert input and pilot testings, the instrument will be created, which is followed by testing of antecedents of technological, organizational and environmental nature using partial least squares structural equation modelling approach. Finally, follow-up of six months will allow exploring whether the readiness at baseline stage predicts future migration action taken by companies.

Anticipated outputs will include readiness index tailored to the particular setting, a body of preliminary evidence regarding PQC readiness of IT firms in India, and understanding the impact of relationships between clients and suppliers on migration. This research aims at bridging the gap between the measure of readiness and organizational action that follows.

Keywords: post-quantum cryptography; organizational readiness; Technology–Organization–Environment framework; crypto-agility; IT services; India

1 Introduction

Public-key cryptography is the basis of several digital services, such as payment authorization, software updates, virtual private networks, and digital signatures. Existing systems use RSA and ECC algorithms whose safety can be threatened if a sufficiently powerful and reliable quantum computer is available. The theoretical basis of such a threat was established by Shor's (1994) algorithm. At present, there is no cryptographically relevant quantum computer (CRQC) but organisations should develop strategies taking into account the fact that data protected now may become accessible in the future because of their confidentiality period (Mosca, 2018; European Telecommunications Standards Institute [ETSI], 2015).

The shift has occurred from algorithm research to implementation. In August 2024, the U.S. National Institute of Standards and Technology (NIST) has completed work on developing three PQC standards: FIPS 203 for ML-KEM, FIPS 204 for ML-DSA, and FIPS 205 for SLH-DSA (NIST, 2024a, 2024b, 2024c). However, even after standardisation, the shift will not become a matter of replacing the old by the new one. Companies need to identify cryptographic uses, prioritise their systems in accordance with data sensitivity and confidentiality lifetime, work together with the application and technology providers, and develop cryptographic agility (Joseph et al., 2022; Barker et al., 2026). The roadmap of India's quantum-safe ecosystem in 2026 is another example of the national policy framework for phased migration and involvement of technology providers (DST Task Force, 2026).

Industry data suggests a mismatch between awareness and preparedness. In a survey of 2,176 IT and security professionals from nine countries, 61% stated that they plan to move to PQC over five years, yet only 41% reported being ready; cryptographic inventory is a major issue for 43%, and 51% reported unclear ownership (Entrust and Ponemon Institute, 2024). In another vendor-sponsored survey conducted among security professionals in the USA, the UK and Australia, only 5% had implemented quantum-safe encryption (DigiCert, 2025). Such industry data, which is neither representative nor indicative of actual readiness levels in India's IT sector, does little more than point to potential gaps in preparedness.

The Indian setting is significant since IT companies offer both technology and managed services to their clients from banking, insurance, healthcare and government sectors. Therefore, IT companies have a dual challenge of securing their cryptographic environment and assisting in migrating to post-quantum cryptography. Thus, organisational readiness may depend on internal organisation-related factors, such as governance, skills and technological capability, along with external factors related to clients' needs and supplier roadmaps. Despite the rise of technical standards and increasing industry interest, empirical studies of PQC readiness in India's IT sector are still scarce, especially considering the mediator position of IT companies.

In this study, it is suggested to develop the PQC Organisational Readiness Index (PORI) as a formative index of firm-level organisational readiness, which would be developed based on organisational readiness theory and Technology-Organisation-Environment framework. Exploratory sequential design of mixed methods research will include interviews aimed at informing instrument development, firm-level survey aiming at understanding firm-level readiness and its determinants, and a six-month follow-up to test if readiness predicts PQC migration activities.

2 Research problem

The main research problem is that there are no adequate empirical studies about the readiness of IT companies operating in India for the migration to post-quantum cryptography (PQC), what factors affect the mentioned phenomenon and whether the readiness leads to the migration process taking place. There are already existing standards on post-quantum cryptography, but the implementation of such standards requires some changes at the level of cryptographic inventories, technical infrastructure, governance, competencies of workforce and suppliers' relations. Thus, the absence of any systematic study of those capabilities can negatively affect investment decisions of IT companies in India.

The problem gets even more acute due to the presence of the threat called 'harvest now, decrypt later'. In this situation, adversaries collect encrypted information in order to decrypt it after the appearance of the necessary quantum computer (ETSI, 2015). As stated by Mosca (2018), the rela-

tion between the period of time for which the data should remain confidential, duration of migration and predicted arrival of cryptographically relevant quantum computer needs to be considered. The migration of the IT service providers could take more time depending on client requests, technology vendor and third party infrastructure used by the company.

There are three research gaps which support this study.

First, empirical gap. The reviewed literature shows that there is no enough firm-level information about PQC readiness and migration activities among IT companies operating in India. There are industry surveys conducted by international organizations that could serve as useful tools, but they are unable to give information about India's IT industry readiness.

Second, conceptual/measurement gap. Post-quantum cryptography readiness requires evaluation of several organizational capabilities. However, the reviewed literature does not show the existence of the validated, specific formative scale that measures PQC readiness and whether it predicts migration behavior.

Third, ecosystem gap. IT service providers act both as the organization which is performing migration and intermediary that helps the client to conduct such migration process. That is why, their readiness could be influenced by the pressure from the client side and dependence on the suppliers and the opposite way around. The mentioned issue was poorly studied within the context of IT companies in India.

The proposed study will close the gaps and develop the PQC Organizational Readiness Index, analyze antecedents (technological, organizational and environmental) and relationship with the migration actions.

3 Research questions and objectives

3.1 Research questions

RQ1: What is the current status of the awareness, organisational readiness and migration activities in relation to PQC among information technology and technology companies based in India and how does this status vary by firm size and sub-sectors within the industry?

RQ2: How far do the factors of technology, organisation and environment account for variation in the organisational readiness for PQC?

RQ3: How far does the organisational readiness for PQC, operationalised through the PQC Organisational Readiness Index (PORI), predict future actions to migrate, after controlling for previous migration actions?

RQ4: How do IT service providers understand their role as intermediaries in helping their clients migrate to PQC and does the relationship between pressure and organisational readiness vary between the two types of firms?

3.2 Research objectives

1. PORI development and validation as a formative, firm-level index of PQC readiness through qualitative analysis, expert evaluation, pilot testing, and quantitative validation, with a specific focus on assessing the predictive validity of the instrument.

2. Building a baseline of PQC awareness, organizational readiness, barriers, and migration activities for IT and technology companies active in India.

3. Analyzing the determinants of PQC readiness and testing the hypotheses about the relationships between managerial threat appraisal, top management support, perceived migration complexity, client pressure, and regulatory pressure with PORI.

4. Testing the predictive validity of PORI and assessing whether baseline readiness predicts migration activities performed six months after that time, adjusting for baseline migration activities.

5. Assessing the intermediary effect of IT services companies on their clients' PQC migration and testing whether client pressure is a stronger determinant of PQC readiness for IT services companies compared to product and platform companies.

4 Literature review

4.1 The quantum threat and the standards landscape

The Shor (1994) algorithm proved that a quantum computer with enough computing capacity can compromise the security of popular public key cryptosystems such as RSA and ECC. Grover's (1996) algorithm is a relatively different threat to symmetric cryptography that has different implications depending on the cryptographic strength and implementation involved. NIST went ahead to develop standards for three PQC algorithms, which are FIPS 203, FIPS 204 and FIPS 205 (NIST, 2024a, 2024b, 2024c). However, standardisation does not solve the problems of migration in operation.

An organisation will be required to assess the cryptographic dependencies, priority of systems based on data sensitivity and confidentiality lifetime, compatibility with vendors, and the implications of interoperability and performance with the new cryptographic algorithms. The literature on organisational transition and cryptographic agility shows that an important factor in migration to PQC is staged migration, adaptability of architectures and the capacity to substitute cryptographic techniques without major system redesign (Joseph et al., 2022; Barker et al., 2026). This suggests that PQC migration is not only a technical problem. It has other organisational aspects, which include governance, resource availability and internal expertise and coordination across organisations.

4.2 Organisational readiness as a construct

Organisational readiness theory provides a foundation for distinguishing preparedness from actual implementation. Armenakis et al. (1993) conceptualise readiness for change through the beliefs and intentions that support organisational change, while Weiner (2009) emphasises collective commitment to change and shared confidence in the organisation's capacity to implement it. In information systems research, Lokuge et al. (2019) demonstrate how readiness for digital innovation can be operationalised through multiple organisational resources and capabilities.

Applied to PQC migration, readiness encompasses both the willingness to undertake the transition and the organisational capacity to execute it. Awareness of quantum risk alone is insufficient if a firm lacks an assigned owner, cryptographic inventory, technical flexibility or trained personnel. This distinction supports measuring readiness separately from migration outcomes.

The proposed PQC Organizational Readiness Index (PORI) extends this reasoning through five dimensions: governance and strategic commitment, cryptographic visibility, technical agility, human capital, and ecosystem coordination. These dimensions represent complementary but distinct capabilities. Formative measurement is therefore appropriate as a proposed specification because a

weakness in one capability is not necessarily offset by strength in another. This approach follows established guidance on formative index construction and the risks of measurement misspecification (Diamantopoulos and Winklhofer, 2001; Jarvis et al., 2003). The proposed instrument must nevertheless establish content validity, measurement quality and predictive validity through the study rather than assume them in advance.

4.3 Theoretical lens: The TOE framework

The Technology–Organisation–Environment (TOE) framework explains firm-level technology adoption through technological characteristics, internal organisational conditions and the external environment (Tornatzky and Fleischer, 1990). Oliveira and Martins (2011) review its use in firm-level information technology adoption, while Hasani et al. (2023) examine organisational cybersecurity adoption and its relationship with organisational performance. Together, this literature supports examining readiness as a product of interacting technological, organisational and environmental conditions.

For PQC migration, perceived complexity represents a potential technological barrier, whereas management support and resource commitment represent organisational enablers. The attention-based view of the firm suggests that managerial attention influences which issues receive organisational resources (Ocasio, 1997), providing a rationale for examining managerial threat appraisal. Institutional theory further explains how powerful external actors influence organisational behaviour through coercive pressures (DiMaggio and Powell, 1983). Applied to this study, client demands and perceived regulatory expectations may motivate firms to prioritise migration before external deadlines become binding.

These perspectives provide complementary explanations for the proposed antecedents of PORI. TOE supplies the overarching adoption framework, while the attention-based and institutional perspectives help explain managerial prioritisation and external pressure. Their relevance to PQC readiness in Indian IT firms remains an empirical question to be tested.

4.4 Empirical evidence on PQC readiness

Available industry surveys indicate a gap between awareness and operational preparation, although their findings require cautious interpretation. Entrust and Ponemon Institute (2024) report concerns about cryptographic inventory and unclear transition ownership among surveyed IT and security professionals. DigiCert (2025) reports limited implementation of quantum-safe encryption, while Capgemini Research Institute (2025) identifies differences in organisational maturity and the development of formal migration programmes. These studies offer useful indicators of perceived industry challenges, but their vendor-sponsored and self-reported nature limits the conclusions that can be drawn about actual readiness across national populations.

Le et al. (2025) synthesise standards, industry surveys and threat intelligence to examine enterprise preparedness. Their review highlights uneven preparation, resource constraints and the importance of early migration planning; however, it should be treated as a synthesis of existing evidence rather than an independent firm-level survey.

More directly, Zimmermann et al. (2025) examine organisational adoption through 14 expert interviews and a survey of 37 cybersecurity professionals. Their study identifies regulatory expectations, risk exposure and reputational considerations as potential adoption drivers, alongside resource limitations, third-party dependencies and cryptographic inventory challenges as barriers. This

research provides an emerging empirical foundation for organisational PQC adoption, but its comparatively small sample does not establish a validated readiness index or a sector-specific baseline for India. The longitudinal relationship between a multidimensional readiness measure and subsequent migration behaviour also remains an important question for the present study.

4.5 Research gap: IT firms as migration intermediaries

India's 2026 quantum-safe migration roadmap establishes a national policy context for cryptographic transition, including the participation of technology providers, vendor engagement and the development of organisational migration capabilities (DST Task Force, 2026). For IT firms operating in India, the challenge is distinctive because they must prepare their own systems while also supporting clients' transitions.

IT services firms occupy an intermediary position between client organisations that specify security requirements and technology suppliers whose products and roadmaps constrain implementation choices. Client pressure may accelerate investment in readiness, while supplier dependencies and limited visibility into client environments may complicate execution. This relationship also creates a potential feedback effect: a service provider's preparedness may influence the migration support it can offer clients, while clients' demands may influence the provider's own priorities.

The literature reviewed therefore suggests three connected research gaps. First, India-specific firm-level evidence on PQC readiness and migration activity remains limited. Second, an empirically assessed formative measure that links organizational capabilities to subsequent migration actions is needed. Third, the intermediary role of IT services firms, including how client pressure relates to readiness across firm types, requires further examination. These gaps motivate the development and assessment of PORI and the proposed mixed-methods.

5 Hypotheses

5.1 Conceptual model and the PORI construct

This study seeks to link organisational readiness theory with the Technology–Organisation–Environment (TOE) approach for explaining variability in post-quantum cryptography (PQC) readiness within IT and technology firms in India. The TOE approach is the overarching theoretical model for exploring antecedents of technology adoption that involve technology, organisational and environmental factors (Tornatzky and Fleischer, 1990). Organisational readiness theory separates the commitment to effect change from the collective capabilities needed to implement it (Weiner, 2009). Attention-based theory and institutional theory provide additional insight into the suggested relationships by helping understand managerial focus and external influences from clients and regulators (Ocasio, 1997; DiMaggio and Powell, 1983).

The focal construct is the PQC Organisational Readiness Index (PORI), operationalised as a company's organisational capability and commitment to detect, prioritise and move away from quantum-vulnerable cryptographic technologies used by itself and associated with the use of relevant technologies. PORI is described as a formative and second-order construct composed of five dimensions of organisational readiness: governance and strategic commitment, cryptographic visibility, technical agility, human capital, and ecosystem coordination. These five dimensions are specific, non-redundant capabilities that together make up PORI (Diamantopoulos and Winklhofer, 2001; Jarvis et al., 2003).

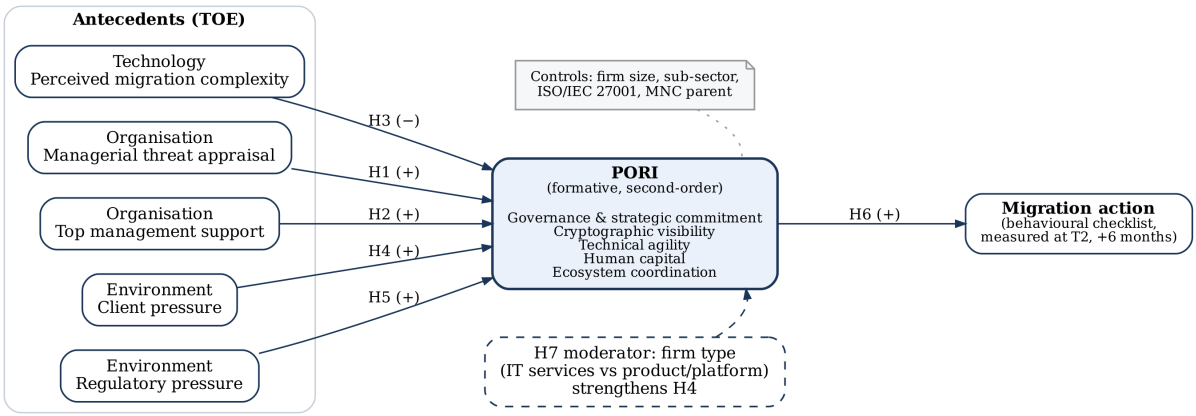

Figure 1. Conceptual model: TOE antecedents of PQC readiness (PORI) and its predicted effect on migration action.

Table 1. PORI dimensions.

Dimension	Definition	Example indicators
Governance and strategic commitment	Ownership, planning and resourcing of the transition at leadership level	Named owner; written roadmap; budget line; PQC in board risk reporting
Cryptographic visibility	Knowledge of where and how cryptography is used across the estate	Inventory coverage; discovery tooling; data classified by confidentiality lifetime
Technical agility	Ability to change algorithms without re-engineering systems	Centralised crypto libraries or PKI; hybrid TLS tested; vendor PQC roadmaps assessed
Human capital	Skills available to plan and execute migration	Trained staff; PQC training programme; access to specialist expertise
Ecosystem coordination	Alignment with clients and suppliers on migration	PQC clauses in procurement; CBOMs requested; client roadmaps discussed

Indicators will be finalised after Phase 1 interviews and expert review.

5.2 Hypotheses

Attention to a remote, uncertain threat hinges on whether its leaders perceive that threat as relevant in the present (Ocasio, 1997). Such leaders' awareness of HNDL risks and regulatory timeframes increases the likelihood of resource allocation.

H1: Managerial threat appraisal is positively correlated with PQC readiness (PORI).

The top management support is one of the most reliable predictors of information security and IT adoption in TOE studies (Hasani et al., 2023; Oliveira and Martins, 2011), and migration entails a cross-functional budget and authority.

H2: Top management support is positively correlated with PORI.

Perceived complexity has long been a conventional technological barrier in TOE research. The larger artefacts of the technology under analysis, mixed modes and vendor dependency (Section 5.1) are conducive to perceived complexity.

H3: Perceived complexity of migration is negatively correlated with PORI.

Regulated sector clients have their own deadlines, and they can make demands upon vendors through contractual relationships, and this constitutes a coercive institutional pressure (DiMaggio and Powell, 1983).

H4: Client pressure for quantum-safe delivery is positively associated with PORI.

The expectations from the Indian roadmap and NIST's transition timelines exist even before they become mandatory through regulatory pressure.

H5: Perceived regulatory pressure is positively associated with PORI.

If PORI really indicates the readiness of a firm, it should be able to predict how firms behave in the future. This is the test for the validity of prediction, which is missing in existing indices.

H6: PORI at T1 is positively associated with migration activities completed by T2 six months later.

Since the services firms have to migrate for their clients, they will be more affected by the client demand compared to other firms selling their own products and platforms.

H7: The positive impact of client pressure on PORI is higher for IT services firms than for product and platform firms.

Size of the firm, subsector, ISO/IEC 27001 certification, and multinational parent are controlled for. Size of the firm was a hypothesis in the previous draft but is now controlled for since its resource slack explanation is well documented and has no theoretical contribution in the current study.

6 Research methodology

6.1 Research design

The study follows a pragmatist, exploratory sequential mixed-methods design (Creswell and Plano Clark, 2018). There is no validated PQC readiness instrument to adopt, and the intermediary role has not been described, so a qualitative phase is needed before measurement. The design has three phases:

Phase 1, qualitative exploration. 12–15 semi-structured interviews with CISOs, security architects and delivery heads, purposively selected across firm sizes and sub-sectors. Interviews explore how firms are approaching PQC, what obstacles they face and how client relationships shape the work. They are analysed by reflexive thematic analysis (Braun and Clarke, 2006).

Phase 2, instrument development. Items are generated from the literature and Phase 1 themes, following established construct-development procedures for information systems research (MacKenzie et al., 2011). A panel of five to six experts drawn from academia and industry rates each item, and content validity ratios are computed (Lawshe, 1975). The instrument is then piloted with about 30 respondents for clarity and timing.

Phase 3, survey and follow-up. Survey and follow up. Cross-sectional survey is conducted at Time 1 to collect data on antecedents and PORI. After six months, the same respondents are asked to complete a behavioural checklist of migration activities (Time 2). The temporal separation between predictors and outcomes will make the H6 test more valid.

6.2 Unit of analysis and sampling

Firm is the unit of analysis. An informant from each firm is the sole representative, and he is a senior security or technology person knowledgeable about cryptographic choices (Kumar et al., 1993). There are two questions on informant competence, and informant answers having little knowledge are eliminated. The sampling universe comprises IT and technology companies with presence in

India through membership of NASSCOM and DSCI, India chapter of ISACA, and $(ISC)^2$ India chapter and professional contacts. Quota sampling is done based on company size (below 2,000 and 2,000 or more) and sub-sector (IT services and outsourcing, software products and platforms, cloud and infrastructure, cybersecurity, and fintech).

As the sample is non-probability, we can draw conclusions based on analytical generalization only. We will make comparisons between the sample profile and that of the sector, and will point out differences instead of estimates at population level.

The sample size is determined based on the needs of the structural model rather than the estimation of proportion formula. According to the Kock and Hadaya (2018), detecting a path coefficient of 0.20 with the inverse square-root approach of PLS-SEM at the 5% level of significance with 80% power demands at least 155 units while 99 units are required for a coefficient of 0.25. Similarly, when computing the same through the G*Power with eight predictors, medium effect of $f^2 = 0.15$, $\alpha = .05$ and 80% power, the estimated minimum sample size is 109 (Faul et al., 2009). Therefore, our target is 150 completed surveys with 100 forming the lower limit. Cold outreach to senior security executives will have low response rate (in the single digits) and, thus, we will have to utilize warm sources (associations, chapter events and alma maters) along with a pool of 1,500 names.

6.3 Instrument

The survey comprises 45 questions and requires about 15 minutes to complete. Section A deals with the personal and company information and informants' competency. Section B includes measurement of the five antecedents using multi-item scales of reflection type based on seven-point agreement scale. Section C deals with the measurement of the five PORI dimensions using four to five formative indicators and one global indicator each ("Our organisation is ready for migration to post-quantum cryptography"). Section D deals with the recording of barriers' severity using five-point scale for descriptive ranking. An item unrelated to theory is used for detecting common method bias. The Time 2 measure consists of about eight tangible and verifiable actions: inventory taken, owner identified, budget approved, PQC requirements incorporated into the procurement process, request for CBOMs sent to vendors, hybrid or PQC TLS implementation tested, staff trained, and client migration engagement planned.

6.4 Bias controls

The single-respondent survey is prone to method bias and socially desirable responses, and there is a chance that the security leader may exaggerate the readiness of their organisation. Solutions at the procedural level include guaranteed anonymity, different scale formats for different sections, behaviorally anchored questions, and assessment of the outcome at a later time (Podsakoff et al., 2003). The statistical solutions are the marker variable approach and VIF test of full collinearity, where any value lower than 3.3 means the absence of significant common method bias (Kock, 2015).

6.5 Ethics and data protection

The research will be approved by the university's research ethics committee prior to data collection. Participation will be on a voluntary basis, consent will be obtained electronically, and no business will be named in any of the outputs. The personal data will consist only of contact information required for the Time 2 survey, which will be collected separately from answers and destroyed after being matched, as prescribed in the Digital Personal Data Protection Act, 2023 (Government of India, 2023).

6.6 Timeline

Table 2. Indicative project timeline.

Months	Activity	Output
1–2	Ethics approval; interview guide; recruitment	Approved protocol
2–4	Phase 1 interviews and thematic analysis	Themes; draft item pool
4–5	Expert review; pilot test	Final instrument
5–7	Phase 3 survey, Time 1	100–150 firm responses
7–9	Measurement and structural model analysis	Validated PORI; H1–H5, H7 results
11–13	Time 2 follow-up and H6 test	Predictive validity result; final report

7 Analysis of the data

7.1 Qualitative analysis

The interview data will then be analyzed inductively to produce themes. These will be compared against the TOE context and PORI framework to generate a description of the intermediary role that contributes towards answering the first part of RQ4..

7.2 Descriptive analysis

Descriptive statistics such as frequency, mean and cross-tabulation will be used to analyze awareness, readiness, barrier and migration activities based on firm size and sub-sector (RQ1). Severity of barriers will be ranked and compared through the use of the Friedman test with post hoc pairwise comparisons. PORI scores will be calculated based on the weights determined for each of the indicators and then rescaled into a range of 0-100.

7.3 Measurement model

The model will be tested in PLS-SEM, which is appropriate for formative constructs, predictive research objectives and moderate sample sizes (Hair et al., 2022). The reflective constructs that serve as antecedents will be tested in terms of factor loadings (≥ 0.708), composite reliability (0.70–0.95), average variance extracted (≥ 0.50) and discriminant validity using HTMT (< 0.85) (Henseler et al., 2015). Convergent validity for the formative PORI construct will be evaluated using redundancy analysis relative to the global readiness item, collinearity (VIF < 3) and the significance and relevance of indicators' weight coefficients via bootstrapping, where 5,000 subsamples will be generated. The second order construct will be tested using disjoint two stage estimation approach (Becker et al., 2012; Sarstedt et al., 2019).

7.4 Structural model and hypothesis testing

H1–H5 will be tested through bootstrapped path coefficients, with R^2 and f^2 reported. Out-of-sample predictive power will be assessed with PLSpredict (Shmueli et al., 2019). H6 will be tested by regressing the Time 2 action count on Time 1 PORI scores, controlling for actions already completed at Time 1. H7 will be tested through multigroup analysis after establishing measurement invariance (Henseler et al., 2016). If subgroups are too small, an interaction term will be used instead. Results will be reported with effect sizes and confidence intervals rather than significance alone.

Table 3. Analysis plan aligned to research questions and hypotheses.

Phase	Method	Question / hypothesis
Qualitative	Reflexive thematic analysis	Item pool; RQ4 (role)
Descriptive	Frequencies, cross-tabulations, Friedman test	RQ1 baseline; barrier ranking
Measurement	PLS-SEM: reflective and formative assessment; two-stage higher-order model	PORI validation
Structural	Bootstrapped paths, R^2, f^2, PLSpredict	RQ2: H1–H5
Predictive	Regression of Time 2 actions on Time 1 PORI	RQ3: H6
Moderation	MICOM and PLS multigroup analysis	RQ4: H7
Typology	Cluster analysis of PORI dimension scores	RQ1 readiness tiers

8 Expected observations, contributions and suggestions

No primary data has yet been collected. This section therefore sets out expectations drawn from the literature and the contributions the study is designed to make. It does not report findings.

8.1 Expected observations

In light of the global evidence, we anticipate that awareness regarding the quantum threat will be high amongst senior security leaders in large organizations and low in mid-sized organizations. We anticipate that full cryptographic inventories will be rare considering inventory is the most commonly reported impediment in global studies (Entrust and Ponemon Institute, 2024) and that India's inventory and CBOM requirements are recent and lacking regulatory backing at the sectoral level. We anticipate that skills and budget will be among the top impediments, and that most companies will view their posture as monitoring the situation rather than preparing actively. More importantly, we anticipate that companies deriving substantial revenues from regulated sectors will be more advanced. Should H4 and H7 prove correct, it appears that client contracts rather than national regulations could drive PQC preparedness in Indian IT in the next few years.

8.2 Intended contributions

Theoretical. The study defines PQC readiness as an organisational construct grounded in readiness theory. It extends TOE to a transition that is mandated, long-horizon and largely invisible to users. It also introduces the intermediary role as a factor in cryptographic migration.

Methodological. It produces a formative readiness index whose predictive validity is tested against later behaviour, which existing maturity models do not offer.

Empirical. It offers a first sector-level baseline for India, a context largely missing from the current evidence.

8.3 Suggestions for enterprise and policy stakeholders

In any case, the existing literature has already shown many actionable recommendations. The companies have to start with cryptography discovery and inventory since none of other actions can even be considered until they accomplish it, which is exactly what India is doing too (DST Task Force, 2026). The companies have to make their architecture crypto-agile and thereby make all changes of

algorithms possible with changes of configurations rather than a whole engineering effort (Barker et al., 2025). The PQC requirements and CBOM request have to be included in procurement before the schedule of vendors becomes a problem. IT service companies have to develop a migration service for clients.

MeitY, along with CERT-In and sectoral regulatory bodies like RBI, SEBI, and TRAI, have a roadmap with milestones but need sector-specific guidance to make them mandatory. A verified readiness tool like PORI can help both regulatory bodies and industry associations to measure their progress.

8.4 Limitations

These sources of bias cannot be totally eliminated, only minimized, by bias control measures. Non-probability sampling means the study's results cannot be generalized statistically. The six months follow-up period might be too short for some migration behaviors to manifest. Lastly, the PQC domain changes rapidly, which means that a baseline taken today will become outdated very fast. This is among the reasons why having a reliable, replicable tool is preferable to taking snapshots.

References

[1] Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NIST IR 8413). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8413

[2] Armenakis, A. A., Harris, S. G., & Mossholder, K. W. (1993). Creating readiness for organizational change. Human Relations, 46(6), 681–703. https://doi.org/10.1177/001872679304600601

[3] Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. Journal of Marketing Research, 14(3), 396–402. https://doi.org/10.1177/002224377701400320

[4] Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W., & Kent, K. (2025). Considerations for achieving crypto agility: Strategies and practices (NIST CSWP 39, updated 2026). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.CSWP.39-upd1

[5] Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. Long Range Planning, 45(5–6), 359–394. https://doi.org/10.1016/j.lrp.2012.10.001

[6] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

[7] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

[8] Capgemini Research Institute. (2025). Future encrypted: Why post-quantum cryptography tops the new cybersecurity agenda. *Capgemini*.

[9] Chaubey, N. K., & Prajapati, B. B. (Eds.). (2020). Quantum cryptography and the future of cyber security. *IGI Global*. https://doi.org/10.4018/978-1-7998-2253-0

[10] Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). *Sage*.

[11] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

[12] Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. Journal of Marketing Research, 38(2), 269–277. https://doi.org/10.1509/jmkr.38.2.269.18845

[13] DigiCert. (2025, May 8). *Quantum readiness gap: A DigiCert study on quantum-safe encryption* [Press release]. https://www.digicert.com/news/quantum-readiness-gap-a-digicert-study-on-quantum-safe-encryption

[14] DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101

[15] DST Task Force. (2026). Implementation of quantum safe ecosystem in India: Report of the task force. *Department of Science and Technology*, Government of India. https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf

[16] Entrust & Ponemon Institute. (2024). 2024 PKI and post-quantum trends study. *Entrust*.

[17] European Telecommunications Standards Institute. (2015). Quantum safe cryptography and security: An introduction, benefits, enablers and challenges (ETSI White Paper No. 8).

[18] Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Behavior Research Methods, 41(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

[19] Government of India. (2023). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Law and Justice.

[20] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (pp. 212–219). https://doi.org/10.1145/237814.237866

[21] Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). *Sage*.

[22] Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3*(5), Article 97. https://doi.org/10.1007/s43546-023-00477-6

[23] Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

[24] Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. International Marketing Review, 33(3), 405–431. https://doi.org/10.1108/IMR-09-2014-0304

[25] Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. Journal of Consumer Research, 30(2), 199–218. https://doi.org/10.1086/376806

[26] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. Nature, 605(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

[27] Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of e-Collaboration, 11(4), 1–10. https://doi.org/10.4018/ijec.2015100101

[28] Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. Information Systems Journal, 28(1), 227–261. https://doi.org/10.1111/isj.12131

[29] Kumar, N., Stern, L. W., & Anderson, J. C. (1993). Conducting interorganizational research using key informants. Academy of Management Journal, 36(6), 1633–1651. https://doi.org/10.2307/256824

[30] Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

[31] Le, T. D., Do, P. H., Dinh, T. D., & Pham, V. D. (2025). Are enterprises ready for quantum-safe cybersecurity? *(arXiv:2509.01731)*. arXiv. https://arxiv.org/abs/2509.01731

[32] Lokuge, S., Sedera, D., Grover, V., & Xu, D. (2019). Organizational readiness for digital innovation: Development and empirical calibration of a construct. Information & Management, 56(3), 445–461. https://doi.org/10.1016/j.im.2018.09.001

[33] MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly, 35(2), 293–334. https://doi.org/10.2307/23044045

[34] Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (NIST IR 8547, initial public draft). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8547.ipd

[35] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

[36] Mosca, M., & Mulholland, J. (2017). A methodology for quantum risk assessment. *Global Risk Institute*.

[37] NASSCOM. (2023). Strategic review 2023 [Press release]. https://nasscom.in/sites/default/files/sr-2023-press-release.pdf

[38] National Institute of Standards and Technology. (2024a). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203

[39] National Institute of Standards and Technology. (2024b). Module-lattice-based digital signature standard (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204

[40] National Institute of Standards and Technology. (2024c). Stateless hash-based digital signature standard (FIPS 205). https://doi.org/10.6028/NIST.FIPS.205

[41] National Institute of Standards and Technology. (2025). Status report on the fourth round of the NIST post-quantum cryptography standardization process (NIST IR 8545). https://doi.org/10.6028/NIST.IR.8545

[42] Ocasio, W. (1997). Towards an attention-based view of the firm. Strategic Management Journal, 18(S1), 187–206.

[43] Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. Electronic Journal of Information Systems Evaluation, 14(1), 110–121.

[44] Ott, D., Peikert, C., & other workshop participants. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility (arXiv:1909.07353). *Computing Community Consortium*. https://arxiv.org/abs/1909.07353

[45] Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

[46] Sarstedt, M., Hair, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. Australasian Marketing Journal, 27(3), 197–211. https://doi.org/10.1016/j.ausmj.2019.05.003

[47] Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. European Journal of Marketing, 53(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189

[48] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

[49] Stebila, D., & Mosca, M. (2017). Post-quantum key exchange for the internet and the Open Quantum Safe project. In R. Avanzi & H. Heys (Eds.), *Selected Areas in Cryptography – SAC 2016* (LNCS 10532, pp. 14–37). Springer. https://doi.org/10.1007/978-3-319-69453-5_2

[50] Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. *Lexington Books*.

[51] Weiner, B. J. (2009). A theory of organizational readiness for change. *Implementation Science, 4*, Article 67. https://doi.org/10.1186/1748-5908-4-67