KQUANTA RESEARCH

WHITEPAPER • POLICY & REGULATORY BRIEF

New Frontiers:
AI + Quantum Technology

Future-Proofing Insurance for Bharat

A policy and governance roadmap for building resilient, inclusive and future-ready insurance in India.

KQUANTA RESEARCH

About This White Paper

This white paper has been developed by Kquanta Research, an Indian financial deep-tech research firm working on artificial intelligence, quantum technology and sustainability, with a particular focus on the BFSI sector.

Our Mission

To close the artificial intelligence and quantum talent and awareness gap, and to help make India more resilient and quantum-awarem, supporting the country's transition to a quantum-ready economy through independent research, policy insight and practical thinking for Bharat.

For Discussion With	India's insurance ecosystem — insurers, reinsurers, actuaries, boards, risk, technology leaders, academia and policymakers
Classification	Insurance Industry White Paper
Publisher	Kquanta Research LLP

This white paper is intended for information and discussion purposes.

Disclaimer

This document is published by Kquanta Research as a contribution to ongoing research and industry dialogue. The findings, interpretations and conclusions expressed herein are those of Kquanta Research and do not represent the views of any regulator, government body or other organisation named or referenced in this paper. Portions of this document, including some images, may have been machine-generated and/or machine-translated. This document is intended for general information and discussion purposes only and should not be treated as legal, regulatory, investment or actuarial advice, nor as a recommendation to buy or sell any security. Kquanta Research makes no warranty, express or implied, and assumes no liability for the accuracy, completeness or usefulness of the information contained herein.

Reproduction & Attribution

Table of Contents

FOREWORD

Shri B. C. Patnaik

Director, National Insurance Academy (NIA), Pune

Insurance is a contractual promise across time. A life policy written today may carry obligations extending thirty or forty years forward; long-term liability and business interruption covers can run into different eras of technology altogether; and a reinsurance treaty depends, for its legal integrity, on records and digital signatures that must remain enforceable for as long as the underlying promise stands. Few industries carry this burden of duration, and it is what makes insurance uniquely accountable over the long run.

This white paper, New Frontiers: Artificial Intelligence + Quantum Technology: Future-Proofing Insurance for Bharat, poses a question: whether the data, models and digital-trust infrastructure underpinning today's insurance promises will remain secure and governable across their intended lifetime. Artificial intelligence is already embedded in Indian insurance (underwriting, pricing, claims, fraud detection), and that growing dependence raises the stakes attached to trusted data and cyber resilience. Quantum technology is a further, more forward-looking frontier, raising long-horizon questions about cryptographic resilience that may in time bear on policy records and digital trust.

Two concepts merit board-level attention: harvest now, decrypt later, and trust now, forge later. Neither requires a precise timeline; both reward proportionate planning. The paper's use of Mosca's theorem as a governance lens is valuable here; where the time data must remain protected, plus the time needed to migrate, could exceed the time before quantum computing becomes a practical threat, a sector may already be inside a meaningful planning window. This is a conversation worth having within ORSA, stress testing and board oversight, as and when insurers judge it relevant to their own exposure.

India is building domestic capability through the National Quantum Mission and the Department of Science and Technology. Indian insurers will, in time, need to build governance and human capital to engage with this intelligently, in service of the sector's own ambition of 'Insurance for All by 2047'.

I welcome Kquanta Research LLP's effort to bring together questions often treated in isolation; artificial intelligence, quantum resilience and long-tail liability and to examine them through the specific lens of Indian insurance. The firm's focus on translating complex technological developments into decision-relevant thinking for boards, actuaries and policymakers reflects a genuine investment in sectoral readiness.

The National Insurance Academy remains committed to this work through building management capacity, driving strategic policy research, cultivating skilled talent and convening structured dialogue for the insurance, pension and allied sectors. Insurance has always been defined by the quality of the promises it keeps. This white paper is a timely and considered contribution to keeping those promises secure over the decades for which they are intended.

AT A GLANCE

Key themes covered in this white paper

AI and Quantum Technology: Implications and Solutions for the Insurance Sector

01

AI IN INSURANCE

- Underwriting and pricing
- Claims management
- Fraud detection
- Customer service
- Risk assessment

02

QUANTUM TECHNOLOGY IN INSURANCE

- Catastrophe modelling
- Portfolio optimisation
- Reinsurance
- Complex risk analytics

03

AI + QUANTUM CONVERGENCE

- Different timelines
- Shared possibilities
- Enhanced analytics and modelling
- Focus on data and digital trust

04

QUANTUM READINESS

- Protect sensitive data
- Build crypto-agility
- Integrate with existing governance
- Prepare for evolving standards

THE SCALE OF INDIA'S INSURANCE SECTOR

FY2024–25

DATA AT RISK

Large volumes of sensitive and long-lived data, including:

- Personal and health information
- Policy documents and claims records
- Reinsurance and actuarial data
- Digital signatures, APIs and models

Data that must remain confidential or trustworthy for many years may be exposed to future risks as cryptographic standards evolve.

THE SOLUTION: A PHASED, RISK-BASED APPROACH

Practical steps for insurers and reinsurers

Understand exposure › Build capability › Test and learn › Integrate governance › Move in phases

A more secure, resilient and trusted insurance ecosystem for India.

1 Executive Summary

STRATEGIC CONTEXT

For India's insurers and reinsurers, artificial intelligence is no longer an emerging technology to plan for. It is already influencing how risk is priced, claims are managed, fraud is detected and customers are served. Quantum computing is on a different trajectory. Potential applications in catastrophe modelling, portfolio optimisation and complex risk analytics are being explored, but the timing and extent of meaningful quantum advantage remain uncertain.

This creates two related but distinct imperatives:

Quantum Advantage — Opportunity	Quantum Readiness — Resilience
▪ Predictive modelling and pricing ▪ Catastrophe and climate analytics ▪ Portfolio and treaty optimisation ▪ Fraud and anomaly detection	▪ Long-term data confidentiality ▪ Protection against 'Harvest Now, Decrypt Later' ▪ Transition to Post-Quantum Cryptography (PQC) ▪ Preservation of digital signatures

WHY INSURANCE IS UNIQUELY EXPOSED

Insurance is, at its core, a long-duration contractual commitment. That duration creates a particular exposure: information, contracts and cryptographic protections established today may need to remain confidential, authentic and legally verifiable for decades.

Exposure	Why It Matters
Multi-decade liabilities	Life and annuity contracts routinely run 30–40 years. Claims records, health data, digital signatures and reinsurance agreements may require protection and legal verifiability across similarly extended periods.
Systemic scale	In FY2024–25, India's insurance sector collected approximately **₹11.9 lakh crore** in premiums and managed approximately **₹74.4 lakh crore** in total sector investments.
'Harvest Now, Decrypt Later'	Sensitive, encrypted information captured today could potentially be retained and decrypted in the future; when sufficiently capable quantum computers emerge.
'Trust Now, Forge Later'	Long-lived digital signatures and cryptographic certificates securing policies, contracts and transactions may require migration as quantum capabilities and cryptographic standards evolve.

> ***Mosca's Theorem: if the period for which information must remain secure, plus the time required to migrate systems, exceeds the time before existing cryptography becomes vulnerable, preparation needs to begin before that vulnerability materialises.***

THE INDIAN POLICY CONTEXT

India is advancing initiatives across quantum technology, AI, data protection and cybersecurity. Together, these provide an increasingly relevant policy and resilience context for the insurance sector.

Framework	Insurance-Sector Relevance
DST Quantum-Safe Roadmap (2026) + National Quantum Mission	Places BFSI within the wider quantum-safe and Critical Information Infrastructure transition and provides a national context for longer-term quantum capability and resilience.
IRDAI Cybersecurity Framework + RBI Q-SAFE	Existing expectations around board oversight, cyber resilience and third-party risk provide governance mechanisms through which cryptographic exposure and quantum-related scenarios can progressively be considered.
DPDP Act 2023 / Rules 2025 + CERT-In	Reinforce obligations around protection of personal data, breach management and cyber-incident reporting, independently of the development timeline for quantum computing.
International direction: NIST, UK NCSC, EU and other jurisdictions	International standards and migration roadmaps increasingly treat post-quantum transition as a multi-year technology and resilience programme.

A PHASED, PROPORTIONATE RESPONSE

Rather than attempting to predict the precise arrival of 'Q-Day', the paper proposes a measured, risk-based approach, integrated where appropriate into existing Enterprise Risk Management, ORSA, cyber-resilience and board oversight mechanisms.

1	**Understand Exposure**	Map long-lived data, cryptographic dependencies, legacy systems and material third-party relationships.
2	**Build Crypto-Agility**	Develop internal capability and the ability to update cryptographic keys, certificates and algorithms with minimal disruption.
3	**Use Existing Governance**	Incorporate relevant quantum scenarios into ORSA, stress testing, technology risk and outsourcing oversight rather than creating a separate governance structure.
4	**Experiment and Learn**	Explore AI, quantum and quantum-inspired applications in catastrophe modelling, fraud analytics and optimisation; where there is a credible business case.
5	**Scale Where Justified**	Progress quantum-safe measures in line with evolving standards, evidence, risk exposure and national policy direction.

CONCLUSION

AI and quantum technology are developing on different timelines. AI is already changing insurance; quantum advantage remains exploratory; and quantum readiness raises longer-term questions of data security, digital trust and institutional resilience.

A phased, collaborative and governance-led approach can enable insurers and reinsurers to use AI responsibly today, explore AI + Quantum opportunities as they mature, and strengthen the resilience of the data, systems and cryptographic infrastructure on which long-duration insurance promises depend. Done well, this can contribute to a more innovative, secure, resilient and trusted Indian insurance ecosystem, supporting the longer-term ambition of 'Insurance for All'.

> ***The leadership question is therefore not simply when quantum capability will arrive, but whether the long-duration promises made today, and the data, digital signatures and systems underpinning them, are being prepared to remain secure and trustworthy as technology evolves.***

2 AI + Quantum in Insurance: A Technical Brief for Risk, Capital and Governance

This section sets out clear definitions of artificial intelligence and quantum technology, tailored to the practical realities of insurance and reinsurance governance.

2.1 Artificial Intelligence in Insurance Today

Artificial intelligence is now a mainstream part of how Indian insurers operate. It has moved well beyond early pilots into embedded use across underwriting, pricing, claims handling, fraud detection, customer engagement, and insurers in a number of markets — India included — are now among the more active enterprise adopters of the technology. These systems support richer, more adaptive decision-making, but they also increase insurers' dependence on high-quality data, resilient digital infrastructure and strong governance around explainability, bias and customer outcomes.

The broader direction of travel is from automation towards prediction and prevention. As AI is combined with richer and more continuous data from telematics, wearables, Internet-of-Things sensors and other real-time sources, insurers may be able to identify emerging risks earlier, refine underwriting and intervene more proactively. McKinsey & Company's September 2026 analysis similarly suggests that continuous monitoring could progressively broaden the insurer's role from primarily paying claims; towards predicting and helping to prevent losses.

Over the remainder of the decade, AI capability is likely to deepen further and become more closely integrated with capital, risk and supervisory frameworks. Quantum and quantum-inspired computing sit at a much earlier stage of adoption, and this paper is careful not to treat the two as running on the same timeline. Quantum-inspired methods — classical algorithms that borrow ideas from quantum computing are already usable today; true quantum advantage, where a quantum computer meaningfully outperforms classical alternatives on a real insurance problem, has not yet been demonstrated at production scale. The remainder of this paper treats artificial intelligence and quantum technology as distinct developments before considering where they may eventually intersect.

2.2 Demystifying Quantum — Quantum 101 for Insurance

Quantum technology is often presented in dense, technical language that can obscure rather than clarify its relevance to boards, regulators and insurance leaders. The core ideas needed for governance and strategic decision-making are simpler than they first appear quantum technologies change how information is computed, communicated, sensed and secured — with potential consequences for risk, capital, solvency and policyholder protection.

This section introduces quantum technology through the lens of its relevance to India's insurance and reinsurance sector, focused on implications for underwriting, capital, cyber resilience and regulatory oversight, and deliberately limits scientific and technical exposition.

2.3 From Classical to Quantum: What Actually Changes?

Classical computers process information using bits that are either 0 or 1. Quantum computers use quantum bits, or qubits, which can exist in combinations of 0 and 1 at the same time (superposition) and can be entangled, meaning the state of one qubit is correlated with another even when physically separated.

Basis of Difference	Classical Computing	Quantum Computing
Operating foundation	Uses bits that are either 0 or 1 at a time	Uses qubits that can represent 0 and 1 simultaneously
Temperature requirements	Operates at room temperature	Typically requires extremely low (superconducting) temperatures
Error rate	Low	Currently high, and an active area of research
Where it may help	General-purpose, day-to-day computation	Selected optimisation, simulation and cryptography problems — subject to continued hardware and algorithmic development

Table 1: Classical and quantum computing, illustrative comparison. Source: adapted from Infosys.

For certain problem types particularly optimisation, simulation and factoring — this structure could in principle allow quantum machines to explore very large solution spaces more efficiently than classical computers, once the technology matures.

For insurance, this distinction matters in four areas that warrant attention today, even though most remain some distance from production-scale use.:

- **Risk and capital modelling.** Quantum and quantum-inspired algorithms are being explored for their potential to speed up Monte Carlo simulation, portfolio optimisation and catastrophe modelling, which could in time support richer scenario sets and a better characterisation of tail risk.
- **Reinsurance and asset-liability management.** Treaty design and asset-liability management are complex optimisation problems; quantum-inspired methods may eventually support more granular and dynamic structures.
- **Cybersecurity.** The same computational power that could help solve useful problems could, if realised at sufficient scale, also be used to break widely deployed encryption schemes such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), which would affect data confidentiality and digital signatures.
- **New risk classes.** Quantum-enabled innovation in other sectors such as logistics, healthcare, materials will in time create new products, business models and systemic interdependencies that flow back into insurance risk pools.

Quantum technology is an evolving computational and security capability that could, over time, influence core areas of insurance, from risk selection and pricing to solvency and policyholder trust, with its applications and capabilities developing progressively.

2.4 Four Pillars of Quantum Technology: An Insurance Lens

Quantum technology is often easiest for insurers to think about through four practical pillars, each at a different stage of maturity and each with distinct insurance-relevant implications:

Pillar	What It Is	Insurance-Relevant Use Cases	Strategic Implications
Quantum Computing	Uses qubits instead of classical bits to explore very large solution spaces more efficiently, for certain problem types, once mature.	Monte Carlo simulation for pricing and reserving; catastrophe and climate-risk modelling; portfolio and ALM optimisation; reinsurance treaty optimisation.	Could, over time, enhance risk and capital analytics and support solvency planning and reinsurance efficiency.
Quantum Communication & Cryptography	Uses quantum effects to create highly secure channels, alongside post-quantum algorithms designed to resist quantum-enabled attacks on today's systems.	Protecting policyholder and claims data over 20–40 year horizons; safeguarding digital signatures on policies and treaties; protecting the integrity of APIs and digital workflows.	A direct response to 'harvest now, decrypt later' risk; likely to require phased migration to post-quantum cryptography over time; an increasingly relevant topic for ORSA, cyber resilience and board risk appetite.
Quantum Sensing	Ultra-sensitive sensors that exploit quantum states to measure physical phenomena more precisely than classical instruments.	Climate and catastrophe risk inputs; industrial and infrastructure monitoring for marine and energy lines; health diagnostics relevant to morbidity, mortality and disability products.	Could improve hazard and exposure data for pricing and reserving, enable more granular India-specific climate models, and open opportunities for new parametric products.
Quantum Materials	Novel materials whose behaviour cannot be explained by classical physics, enabling new devices and infrastructure.	New insurable assets across energy, transport and infrastructure; changing loss profiles in industrial and large-commercial lines.	May in time require refreshed technical underwriting expertise and introduce new accumulation and systemic-risk patterns linked to India's industrial and climate-transition agenda.

Table 2: The four pillars of quantum technology — an insurance lens.

2.5 The Two Sides of AI + Quantum Convergence

Artificial intelligence and quantum technology interact in two important ways for insurance governance, and the two sit at very different levels of certainty.

As AI becomes more deeply embedded in underwriting, pricing, claims and risk assessment, as discussed in Section 2.1, insurers become correspondingly more dependent on the integrity, availability and security of the data and digital infrastructure that support these models. This growing reliance is what connects AI adoption to the questions of digital trust, cyber resilience and, ultimately, quantum readiness.

On the upside, quantum and quantum-inspired methods could, as they mature, accelerate some of the most computation-intensive elements of AI-driven risk and capital models — potentially enabling richer scenario sets, more realistic tail-risk characterisation and better treatment of dependencies in solvency calculations.

On the resilience side, sufficiently capable quantum computers could, over time, weaken the cryptography that protects sensitive data, digital signatures, APIs and AI-enabled systems.

This asymmetry provides a practical reason for quantum readiness to be considered at board level now. The potential benefits of quantum computing for areas such as underwriting or capital modelling remain exploratory and will depend on how the technology develops.

The resilience question follows a different timeline. Data captured today could potentially be exposed in the future through ‘harvest now, decrypt later’, regardless of when commercially useful quantum applications emerge in insurance. This reinforces the case for treating quantum readiness not as a separate technology programme, but as an extension of existing cyber-resilience and risk governance, including ORSA, and alongside insurers’ obligations under the DPDP Act, 2023 and CERT-In’s incident-reporting framework.

For boards, chief risk officers, chief actuaries, chief technology officers, chief information security officers and supervisors, the central question is what these developments could mean for risk, resilience and institutional readiness. In particular, it is how AI and quantum technology, individually and together, could reshape assumptions underpinning risk, capital, solvency and governance, including ORSA, internal models, cyber resilience, outsourcing oversight and the long-term protection of policyholders.

3 India's Quantum-Technology Moment and National Roadmaps

3.1 National Quantum Mission and Quantum Valleys

The National Quantum Mission (NQM) sets out India's ambition to develop quantum computing, communication, sensing and materials capability. Its goals include building intermediate-scale quantum computers, deploying quantum communication networks and creating 'quantum valleys' where government, academia and industry can collaborate on applications, including in financial services.

Amaravati Quantum Valley is the flagship hub under this mission. The launch of India's first quantum computer in Amaravati in April 2026 marked a visible shift from roadmap to live domestic infrastructure. For insurance and reinsurance, this signals that quantum technology will be developed and tested inside India's own market within this decade, not observed only at a distance, even if the pace at which it becomes commercially relevant to insurance remains to be seen.

3.2 DST Quantum-Safe Ecosystem Roadmap

The Department of Science and Technology's quantum-safe ecosystem roadmap offers an important national reference point for India's transition towards quantum-resilient digital infrastructure. Its phased approach suggests that quantum readiness could reasonably begin well before cryptographically relevant quantum computers exist, starting with understanding exposure and building the capability to migrate.

For insurers and reinsurers, this is particularly relevant because long-lived policyholder data, digital identities, claims records, actuarial information and interconnected third-party systems may need to remain secure for decades. Viewed through an insurance lens, the DST roadmap's phased structure points away from the unanswerable question of when a cryptographically relevant quantum computer will arrive, and towards a more immediate governance question: are insurers building a clear enough picture of today's cryptographic dependencies to be ready to migrate when the time comes?

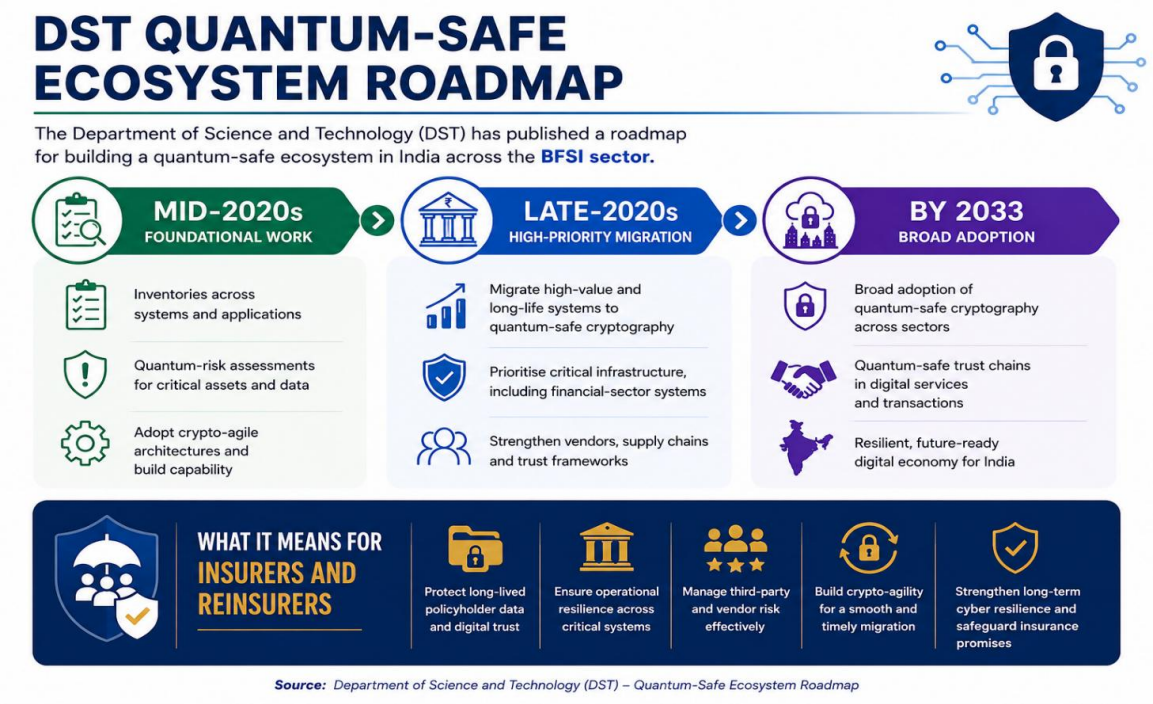


Figure 1: DST quantum-safe ecosystem roadmap for India's BFSI sector. Source: Department of Science and Technology.

3.3 India's Evolving BFSI Quantum-Safe Landscape

IRDAI's Information and Cyber Security Guidelines (2023, revised April 2026) require board oversight, continuous monitoring, third-party risk management and incident response across regulated entities. These provisions do not yet explicitly address quantum-related risk; they do, however, already establish much of the governance infrastructure insurers would need for cryptographic inventory and crypto-agility, should quantum-specific expectations be introduced at a later stage.

At the system level, the Reserve Bank of India's Q-SAFE Expert Committee, constituted in May 2026, has been tasked with assessing the financial sector's cryptographic exposure and developing a roadmap towards a quantum-secure financial system, one insurers may in time be drawn into, given the sector's interconnection with banking, payments and reinsurance markets.

SEBI's Cyber Security and Cyber Resilience Framework (2024) imposes comparable requirements on securities market participants, while MeitY continues to advance cryptographic innovation through regulatory sandboxes and indigenous security capability-building.

Taken together, IRDAI's cybersecurity guidelines, the National Quantum Mission, the DST roadmap and MeitY's agenda form a broader policy landscape within which insurance and reinsurance clearly sit, even though these initiatives are yet to be brought together within a single, integrated framework.

One reasonable reading of regulatory and industry developments, in India and internationally, is that early consideration of post-quantum migration may be useful; well ahead of any definitive quantum-computing threshold. For insurers, this could include progressively developing a clearer understanding of long-lived policyholder data, critical systems and third-party dependencies, proportionate to their own risk profile and exposure.

DPDP and Quantum-Safe Readiness: Distinct Timelines, Shared Resilience

India's Digital Personal Data Protection Act, 2023 is being operationalised through the DPDP Rules, 2025 (G.S.R. 846(E)), notified by MeitY on 13 November 2025, with key obligations phased in over eighteen months. Separately, DST's Implementation of Quantum Safe Ecosystem in India (February 2026) sets out a roadmap towards quantum resilience for Critical Information Infrastructure by 2029 and wider enterprise migration by 2033.

The two frameworks start from different places: one is a statutory data-protection regime, the other a national technology roadmap. But they share an important area of overlap, the long-term protection of data and the cryptographic infrastructure that protection depends on. Neither framework currently cross-references the other, and nothing requires DPDP compliance and quantum-safe migration to be planned as a single programme. That gives insurers and reinsurers room to consider the two together where it is useful to do so, particularly where personal data needs to remain protected over long policy, claims and retention periods.

3.4 An International Comparator: The European Union

The European Union's experience is considered here as one of several international reference points, offering useful context rather than a model for replication. It is useful chiefly because EU policy has, over time, connected data protection, cyber risk, operational resilience, solvency and quantum readiness into five distinct layers, each supervised by a different authority:

- **GDPR — Data Protection.** Sets requirements for the lawful and secure handling of personal data (Regulation (EU) 2016/679, 2016) — broadly comparable in purpose to India's DPDP Act, 2023.
- **EIOPA — Cyber Risk.** The European Insurance and Occupational Pensions Authority's Cyber Risk for Insurers — Challenges and Opportunities (2019) assesses cyber risk across insurers' operations and underwriting.
- **DORA — Operational Resilience.** The Digital Operational Resilience Act (Regulation (EU) 2022/2554, 2022) sets binding ICT risk-management, incident-reporting and third-party-oversight requirements for financial entities, including insurers.
- **Solvency II — Risk Management.** Supplies the broader prudential risk-management and capital framework (Directive 2009/138/EC, 2009) into which cyber and operational risk are integrated.
- **EU Quantum Policy — an Emerging Layer.** Since the European Commission's April 2024 Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, followed by Member States' own coordinated roadmap in June 2025, this layer has moved from concept towards concrete form, addressing future cryptographic risk and the sector's transition towards post-quantum security.

EIOPA's own supervisory work illustrates why this integration matters in practice. In its Report on the Digitalisation of the European Insurance Sector (30 April 2024), EIOPA records that some undertakings already regard the GDPR as 'not sufficiently flexible to address new technologies such as AI or quantum computing, which can infer personal information by combining anonymised datasets' — an acknowledgement that data-protection law drafted before the quantum era may benefit from a forward-looking reading, a point with some resonance for how the DPDP Act, 2023 might be interpreted over time. EIOPA's Methodological Principles of Insurance Stress Testing — Cyber Component (11 July 2023) similarly sets out how a severe but plausible cyber incident could

be translated into capital and solvency impact, an approach that may offer Indian insurers and IRDAI a useful reference point for their own ORSA and stress-testing thinking.

For India, a useful aspect of the EU experience is its sequencing: data protection, cyber-risk assessment, operational resilience and prudential risk management developed as distinct layers, with quantum-specific considerations emerging within this broader framework.

A More Resilient European Insurance Sector

Layering the General Data Protection Regulation (GDPR); EIOPA's cyber-risk assessment and supervisory expectations; the Digital Operational Resilience Act (DORA); the Solvency II prudential framework, including its governance, risk-management and own-risk assessment requirements; and an emerging EU quantum-policy and quantum-safe cybersecurity layer is intended, over time, to produce a stronger combined outcome: robust protection of personal data, cyber resilience, operational continuity and long-term policyholder and market trust.

Figure 2: The EU's layered regulatory approach to insurance — from GDPR and EIOPA's cyber-risk assessment, through DORA and Solvency II, to an emerging EU quantum-policy layer. Source: adapted from EIOPA publications; see References.

3.5 Global Quantum Readiness Standards: Implications for Financial Services

Beyond the European Union, several standards bodies, central banks and financial supervisors have begun to define what quantum readiness means in practice for their own sectors. These initiatives do not add up to a single, unified global standard, and most are not binding on Indian insurers. Read together, however, they show a broad international direction of travel against which India's own roadmap can usefully be read.

- **NIST post-quantum cryptography standards.** The United States' National Institute of Standards and Technology finalised its first three post-quantum cryptographic standards, FIPS 203, FIPS 204 and FIPS 205, in August 2024 — giving industry concrete algorithms to migrate to, rather than a specification still under development. These standards sit behind much of the post-quantum guidance referenced elsewhere in this paper, including NIST IR 8547's proposed timeline for retiring RSA and elliptic-curve cryptography.
- **UK National Cyber Security Centre migration timeline.** The NCSC has set three milestones for large organisations and critical-infrastructure operators: complete discovery and an initial migration plan by 2028; complete the highest-priority migration activity by 2031; and complete migration of all systems, services and products by 2035.
- **G7 Cyber Expert Group roadmap.** In January 2026, G7's Cyber Expert Group published a roadmap intended to encourage a coordinated approach to post-quantum migration across the financial sector. It is explicit that it does not set regulatory expectations of its own, but recommends a risk-based approach, with critical systems addressed around 2030–32 and a general migration target of 2035.
- **Monetary Authority of Singapore.** In July 2026, MAS announced it would issue supervisory expectations later this year for financial institutions to build cryptographic asset inventories, prioritise migration of vulnerable systems and work towards quantum resilience by the end of the decade.
- **Bank for International Settlements.** BIS Papers No. 149, sets out both the opportunities quantum computing may offer central banks and financial institutions and the risks it poses to widely used cryptography, and describes Project Leap, a joint initiative of the BIS Innovation Hub, the Banque de France and the Deutsche Bundesbank exploring practical post-quantum migration for the financial sector.
- **ETSI quantum-safe standards.** The European Telecommunications Standards Institute published a quantum-safe hybrid key-exchange standard, TS 104 015, in March 2025, adding a further technical building block to the post-quantum toolkit available to critical-infrastructure operators, financial institutions among them.

Read together, these initiatives suggest a rough international sequencing: publish algorithms and standards (largely complete by 2024–25); set supervisory expectations and risk-based migration timelines (under way through 2026); prioritise critical systems in the early 2030s; and complete broader migration by around 2035. India's DST roadmap, with a 2029 milestone for Critical Information Infrastructure and 2033 for wider enterprise migration, sits comfortably within this sequencing and, on critical infrastructure specifically, compares favourably with the equivalent milestones set by the UK and the G7.

For Indian insurers, the practical implication is twofold. First, quantum readiness is not a peculiarly Indian concern arriving ahead of its time: comparable financial supervisors elsewhere are moving on broadly similar timelines.

Second, none of the standards above yet impose requirements directly on Indian insurers, so their relevance today lies in showing what good practice is coming to look like internationally, rather than in any compliance obligation of their own. For Indian insurers already reflecting quantum-related scenarios in ORSA, as Sections 4.3 and 5.3 discuss, this international landscape offers a useful external reference point for calibrating those scenarios.

4 Why Indian Insurance and Reinsurance Are Uniquely Exposed

4.1 Long-Tailed Data and Long-Tail Liabilities

Insurance and reinsurance are structurally exposed to quantum-related risk because of duration. Indian insurers and reinsurers manage long-duration life and annuity contracts, often spanning 20-40 years; health and medical data retained well beyond treatment and settlement; long-tail liability and commercial claims with multi-decade resolution horizons; and extensive KYC, identity, income and behavioural data linked to households and firms across the country. This data must remain confidential, authentic and operationally available for decades — a cryptographic scheme updated today may still be responsible for records that need full legal, actuarial and operational value over a 20-40 year horizon.

The reach of insurance-linked protection reinforces this scale. Ayushman Bharat – Pradhan Mantri Jan Arogya Yojana (AB-PMJAY) had generated 43.52 crore Ayushman cards as of 28 February 2026, providing health cover of ₹5 lakh per family per year for secondary and tertiary hospitalisation to around 12 crore families, since extended to approximately six crore senior citizens, and had supported 11.69 crore authorised hospital admissions amounting to ₹1.73 lakh crore. Each of these records, enrolment, eligibility, treatment and claims data; sits within the same long-retention, quantum-relevant category as the policyholder data described above and illustrates why the scale and reach of India's insurance-linked protection ecosystem, beyond headline market figures, are relevant to long-term cryptographic planning.

This is digital personal data under the DPDP Act, 2023, and it therefore engages the Act's retention and erasure requirements. Section 8(7) requires personal data to be erased when consent is withdrawn or when the specified purpose can reasonably be assumed to no longer be served, unless retention is necessary for compliance with law; Rule 8 sets out further retention and erasure requirements for specified circumstances. For insurers, the practical issue is less about shorter retention than about defensible retention — understanding what data is held, for how long, for what purpose, and on what legal or regulatory basis it continues to be held, given that policyholder and claims data legitimately needs to be kept for extended periods for statutory, contractual, actuarial, reinsurance or claims-management reasons. That mapping exercise also has a quantum dimension. Purpose-limited erasure and data minimisation reduce the volume and duration of sensitive information exposed to 'harvest now, decrypt later' risk, but they do not remove the risk attached to information that legitimately needs to stay protected for a long time.

Two distinct cryptographic exposures follow: confidentiality (encrypted data captured today could be decrypted in future, once sufficiently capable quantum computers exist), and authenticity and integrity (digital signatures and other trust mechanisms based on quantum-vulnerable public-key cryptography may eventually need to migrate to quantum-safe alternatives). Neither can be solved through deletion alone; both are cryptographic-lifecycle questions about where vulnerable cryptography sits, how long information must stay protected, and when migration should realistically begin.

This lifecycle framing is consistent with how some European data-protection authorities are approaching the same question.

Italy's data protection authority, the Garante, warns that guaranteed data confidentiality must outlast the lifespan of the encryption currently used to secure it. To maintain GDPR compliance against future quantum decryption threats, organisations must implement crypto-agility alongside NIST-standardised post-quantum algorithms and strict data lifecycle controls. For insurers, data retention and post-quantum migration can be viewed as related parts of managing data securely throughout its lifecycle.

4.2 Harvest Now, Decrypt Later — and Trust Now, Forge Later

Quantum-related risk for insurance has two distinct and compounding dimensions.

Harvest now, decrypt later

Adversaries can steal encrypted data today, store it, and wait until quantum-enabled attacks make it decryptable. For life, health and long-tail general insurance, this could expose policyholders and claims data long after collection, with no opportunity for retrospective protection.

Trust now, forge later

The sector relies on digital signatures, certificates and public-key infrastructure to validate policies, claims, reinsurance treaties, APIs and regulatory records. A sufficiently capable quantum computer could, in time, undermine those signature schemes — raising the prospect that records appearing trustworthy today might later become forgeable, repudiable or legally contestable.

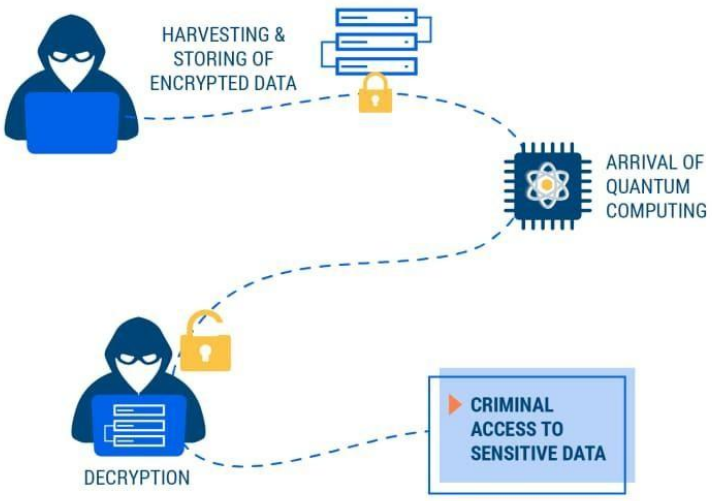


Figure 3: The 'harvest now, decrypt later' pattern — data harvested and stored today could be decrypted once cryptographically relevant quantum computing exists.

Together, these two patterns show that quantum-related risk is not only a privacy concern. It touches legal enforceability, operational continuity and long-term institutional trust, all foundational to the insurance covenant with policyholders.

'Q-Day' is commonly used to describe the point at which a sufficiently capable quantum computer could compromise widely used public-key cryptography, such as RSA and ECC. It is a planning concept rather than a predicted date, and its timing remains difficult to determine. Several regulators and standards bodies have therefore established migration timelines without seeking to predict precisely when Q-Day might occur.

For insurers, the practical implication of 'harvest now, decrypt later' is that Q-Day's precise date matters less than whether data harvested well before it arrives will still need protecting when it does — which, for the multi-decade records described in Section 4.1, is often already the case.

This long-horizon exposure also sits alongside India's existing cyber-incident reporting requirements. Under CERT-In's Directions of 28 April 2022, specified cyber incidents, including data breaches and data leaks, are subject to a six-hour reporting window from the time they are noticed. Where complete information is not immediately available, the information available at the time may be reported first, with further details provided subsequently. For insurers, this places the protection of long-lived policyholder data within the broader context of established monitoring, incident-response and reporting arrangements.

The DPDP framework and quantum readiness therefore address different dimensions of the same underlying question: whether personal data stays adequately protected throughout its lifecycle.

4.3 Mosca's Theorem as a Governance and Solvency Lens

Mosca's theorem offers a concise way of framing quantum-related governance risk. In plain terms: take X, the length of time data and systems must remain secure; add Y, the time needed to migrate to quantum-safe cryptography; and compare the sum with Q, the time before quantum-enabled attacks might become practical. Where X plus Y is likely to exceed Q, an organisation may have less time to prepare than might initially appear, even though Q itself cannot be predicted with confidence.

Variable	What It Represents	Illustrative Insurance Example
X — Shelf life of data	How long the information must remain confidential or authentic	A health or life policy where medical records, claims history and personal data may need protection for 20–40 years
Y — Migration time	How long it would realistically take to move systems, keys and certificates to quantum-safe cryptography	Insurers with legacy core systems, multiple vendors and long-dated contracts may need 5–10 years or more to complete migration once it begins
Q — Time to quantum threat	The (uncertain) time before a quantum computer capable of breaking today's encryption at scale might exist	Estimates vary widely across credible sources and continue to shift as the technology develops

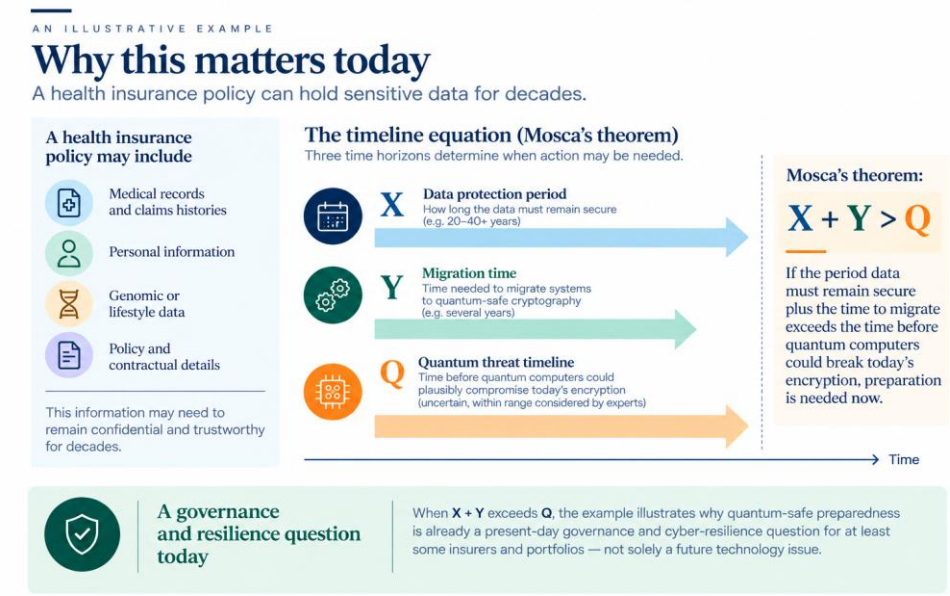
Table 3: Mosca's theorem (X + Y compared with Q) as a governance lens — illustrative, not predictive.

For IRDAI and insurers, Mosca's theorem may also offer a useful lens for considering solvency and ORSA. Where quantum-related risks are considered relevant over the life of long-tail liabilities, they could be considered, where appropriate, within existing approaches to scenario analysis, stress testing, capital planning and recovery planning, alongside broader technology and cyber-resilience considerations.

The DPDP Rules, 2025 add a more immediate dimension to this discussion, with defined breach-notification requirements to the Data Protection Board of India and affected individuals. That means the consequences of a cryptographic or data-integrity failure are not purely a future quantum scenario — they already connect to a present statutory reporting obligation that boards and ORSA processes may find worth rehearsing regardless of how quantum timelines evolve.

External legal and market commentary reaches a broadly similar conclusion from a different direction. Hogan Lovells Cadwalader's May 2026 analysis of quantum risk for insurers describes it as a "slow burning but potentially significant risk" and points to three areas that UK and EU regulators are already watching: data protection (the encryption longevity of customer, claims, health and underwriting data); operational and contractual risk (long-term technology and outsourcing agreements that assume today's security standards will remain effective indefinitely); and governance risk (an expectation of forward-looking, board-level resilience planning, even ahead of any formal quantum-safe mandate).

One approach insurers may wish to consider is a distinct quantum-related cryptographic scenario within ORSA, alongside broader cyber-risk scenarios. This could include assumptions around X, Y and the period over which outsourcing, cloud and reinsurance arrangements rely on current encryption standards. Where contracts do not address potential cryptographic obsolescence, this could also be considered within the insurer's broader risk assessment and board-level discussions, subject to each insurer's own circumstances and judgement. Consider a health insurance policy. Medical records, claims histories and personal data may need to remain confidential for decades. If the period the data must remain secure (X), plus the time needed to migrate systems (Y), exceeds the time before current encryption could become vulnerable (Q), quantum readiness becomes a present-day governance and cyber-resilience consideration.



5 AI + Quantum Technologies: Opportunity and Risk for Insurers and Reinsurers

5.1 Artificial Intelligence in Insurance Today

Artificial intelligence and advanced analytics already play a significant and growing role in Indian insurance, including risk-based pricing and underwriting, automated claims triage, document processing, fraud detection, digital distribution, customer service and portfolio management. The sector is therefore already operating in an increasingly AI-enabled environment.

Recent industry research suggests that AI's role in insurance is moving beyond discrete automation towards deeper changes in underwriting, claims, distribution, servicing and risk prevention. McKinsey & Company (2026), in How AI Will Reshape the Economics of Insurance: A CEO's Guide to Strategy, examines how AI could reshape aspects of insurance economics and support a shift towards more proactive risk identification and prevention.

Boston Consulting Group's 2026 studies, The AI-First Property and Casualty Insurer and The AI-First Life Insurance Company, similarly consider how AI could become more deeply embedded across end-to-end insurance workflows, while retaining human judgement and oversight for exceptions and higher-impact decisions. For insurers, the implications therefore extend beyond efficiency: as AI becomes more embedded in core processes, data quality, model governance, technology architecture, skills and human oversight become increasingly important considerations for management and boards.

Against this backdrop, it is important to distinguish the different trajectories of AI and quantum technology. AI is already influencing operational and strategic decisions across insurance, whereas quantum applications remain at an earlier stage of development. Emerging research nevertheless provides early indications of how quantum approaches might be explored in an insurance context.

A 2026 study published in Springer Nature's Discover Quantum Science, "Motor Insurance Data Analysis by Quantum Machine Learning", provides one such example, applying quantum reservoir computing to motor-insurance claims data and benchmarking the approach against established classical machine-learning techniques. Importantly, the quantum component was implemented using a simulator on classical hardware rather than demonstrating production-scale quantum advantage.

The distinction is important: AI is already a business and governance consideration for insurers, while quantum and quantum-inspired approaches remain areas for targeted experimentation, capability-building and evidence generation as the technology matures.

5.2 Quantum Technology as Risk and Capital Accelerants

A Four-Question Framework

In India, quantum-enabled risk analytics, portfolio optimisation and post-quantum cyber resilience could, over time, help narrow protection gaps in life, health, agriculture, MSME and cyber lines — provided the underlying technology and business case materialise on a useful timeline.

The macroeconomic case for closing these protection gaps is not confined to the insurance sector itself. Lloyd's City Risk Index research states that a one-percentage-point rise in insurance penetration

is associated with additional investment equivalent to roughly 2 per cent of GDP, alongside a reported thirteen per cent reduction in uninsured losses, and a 22 per cent reduction in the taxpayers' contribution following a disaster. Where quantum-enabled analytics eventually help make difficult-to-price risks more insurable at scale, the potential benefits could extend beyond the insurance sector itself.

The table below applies four consistent questions to each area where quantum and quantum-inspired computing are most discussed in insurance: what could change, the potential value, the potential risk, and what is sensible to do now, regardless of how quickly the underlying technology matures.

Topic	What Could Change	Potential Value	Potential Risk	Sensible to Do Now
Underwriting & pricing	Richer, more granular risk analytics drawing on larger and more complex data sets.	Potentially sharper risk differentiation and pricing for previously hard-to-model risks.	Overreliance on unproven models; explainability and fairness challenges if adopted before it is well understood.	Build data quality and model-governance foundations now; treat quantum-inspired tools as an extension of existing AI governance, not a separate track.
Catastrophe & climate modelling	Larger, more granular scenario sets for climate and catastrophe risk.	Better tail-risk characterisation for property, agriculture and climate-exposed portfolios.	False confidence in model outputs that have not been validated against real events.	Pilot quantum-inspired scenario generation.
Asset-liability management	More dynamic optimisation of assets against long-dated liabilities.	Potentially more efficient capital allocation and better-matched portfolios.	Optimisation on flawed assumptions can scale errors quickly across a large book.	Strengthen classical ALM governance first; treat quantum-inspired solvers as a supplementary lens, benchmarked against current methods.
Reinsurance treaty optimisation	More granular, dynamic treaty design across complex, interdependent structures.	Potentially more efficient reinsurance spend and better-structured programmes.	Model risk from opaque optimisation outputs that are hard to explain to boards or regulators.	Use quantum-inspired solvers for exploratory analysis.
Fraud & anomaly detection	Faster pattern-detection across larger, more complex data sets.	Reduced leakage in high-fraud lines such as health, motor and commercial.	False positives affecting genuine claims; privacy and fairness concerns if poorly governed.	Extend existing AI-based fraud analytics; pilot quantum-inspired approaches in sandboxes with clear audit trails.
Capital efficiency & solvency	Richer scenario sets and better dependency modelling in internal-model-style approaches.	More realistic capital assessment and potentially more efficient capital use.	Complexity that outpaces the ability of risk teams and supervisors to validate results.	Keep pace between model sophistication and governance capability; document assumptions transparently.

Long-tail liabilities	Better characterisation of multi-decade reserving and liability risk.	Improved reserving accuracy for liability, health and long-duration life business.	Data and cryptography protecting these liabilities may need to remain secure for longer than any model's planning horizon.	Map long-lived data and its cryptographic dependencies now, independent of modelling ambitions.
Digital trust & cryptography	A gradual shift towards quantum-safe cryptography and crypto-agile architecture.	Continued confidence in digital signatures, policy records and API integrity over decades.	Harvest now, decrypt later; trust now, forge later — both discussed in Section 4.	Begin cryptographic discovery and vendor dialogue now; this is largely a hygiene exercise.
Cyber resilience	A more integrated view of AI, quantum and conventional cyber risk as one risk surface.	Stronger resilience against an evolving threat landscape, including AI-assisted attacks.	Accumulation risk where many insurers and their customers share the same cloud and software dependencies.	Extend existing cyber-resilience frameworks to explicitly consider quantum-era and AI-assisted scenarios.

Table 4: A four-question framework for AI and quantum topics in insurance. None of these applications should be read as implying that quantum computing has already demonstrated a proven advantage over classical methods for these problems — most remain exploratory.

The German Insurance Association (GDV) reaches a broadly similar view in its own position paper on quantum computing and insurance, describing the technology's potential customer-facing upside in comparable terms: fairer, more tailored pricing from richer risk analysis, faster resolution of catastrophic claims, and expanded insurability of previously hard-to-price risks. GDV also calls for EU-level standardisation of post-quantum migration ahead of quantum computers reaching commercial maturity. The same sequencing logic, standardising ahead of commercial maturity rather than after it, arguably applies to India's own quantum-safe transition.

5.3 Implications for Solvency and Internal Models

These developments are relevant to solvency supervision as it stands today. As the Indian market moves towards more risk-sensitive approaches to solvency and enterprise risk management, stochastic modelling, scenario analysis and more sophisticated risk analytics are likely to assume greater importance. Artificial intelligence and quantum-inspired methods could, over time, support richer scenario sets, better tail-risk characterisation and more realistic treatment of dependencies in these calculations.

This reinforces the governance lens set out in Section 4.3: quantum-related cryptographic risk, where material to an insurer's own risk profile, sits naturally within ORSA, scenario analysis and capital-planning discussions, particularly for long-tail lines, rather than as a separate reporting track. Considering it alongside DPDP compliance, including breach notification, may make both easier to manage in practice, though the right structure will differ across institutions.

5.4 One Risk Surface: Data, Models and Cryptography

Artificial intelligence, quantum technology and cyber risk are best understood as one integrated risk surface rather than three separate programmes: quantum-safe migration decisions will determine which AI systems and data sets remain defensible over long horizons. AI itself can also help by inventorying cryptographic exposure, detecting anomalies, and simulating quantum-related cyber scenarios for ORSA and governance purposes.

CERT-In's cybersecurity framework reinforces this integrated view. Its 25 May 2026 Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure emphasises continuous exposure management, rapid remediation, monitoring, identity governance and operational resilience. For insurers, these principles matter because a quantum-era cryptographic failure or an AI-enabled cyberattack could simultaneously become a data-protection, operational, model-integrity and policyholder-protection event — which is also why the six-hour reporting window under CERT-In's 2022 Directions is relevant: an insurer's ability to identify, contain and report an incident quickly is itself part of its overall resilience.

Figure 4: Ransomware trends, 2026. Source: Insurance Thought Leadership, drawing on US FBI data for 2025.

Market data on ransomware helps explain why this belongs in capital modelling and not only in operational risk registers. Insurance Thought Leadership's 2026 review of ransomware trends notes that attacks have moved beyond simple encryption toward credential theft, cloud-infrastructure compromise and attacks on backup and recovery systems themselves — with the US FBI recording 3,611 ransomware complaints and USD 32.3 million in reported losses in 2025, and 63 new ransomware variants emerging that year.

The more significant point for insurers is accumulation risk: because many organisations share the same cloud providers, software dependencies and AI platforms, a single compromised dependency can generate correlated losses across an entire portfolio at once, what the review terms "serial cyber catastrophes." A quantum-enabled cryptographic failure could behave similarly, though potentially at greater scale and across longer-lived data.

In ORSA scenario design, it is worth looking beyond individual exposure to portfolio- and reinsurance-level accumulation from a shared cryptographic or third-party failure, alongside the data-protection and cyber-incident scenarios already discussed above.

This capability base provides a foundation for measured and proportionate preparation, with governance evolving alongside the technology and its applications.

6 Sandboxes and a Quantum-Ready Roadmap

6.1 Sandboxes as AI + Quantum Insurance Laboratories

Regulatory sandboxes are already an established mechanism for supervised innovation in Indian insurance. Earlier IRDAI cohorts have enabled usage-based motor, wellness-linked health products and app-based claims journeys to be tested under controlled conditions, showing that structured experimentation can expand market possibilities without weakening supervisory safeguards.

Artificial intelligence and quantum technology may benefit from a similar approach. Their potential upside in risk analytics, capital efficiency and cyber resilience is significant, but so are the solvency, conduct and systemic-risk questions they raise. A sandbox-centred 'test-learn-consider' cycle offers one practical way to understand these technologies under live conditions while keeping risk contained.

6.2 Priority Themes for AI + Quantum Insurance Sandboxes

AI + Quantum-Enhanced Fraud and Anomaly Detection

- Focus on high-risk lines such as health, motor and commercial, where fraud and leakage are material.
- Build in strong expectations on fairness, explainability, privacy and cyber resilience, including clear model documentation, bias checks and audit trails.

Post-Quantum Cryptography (PQC) and Crypto-Agility Pilots

- Target critical workflows: policy issuance, endorsements, claims, reinsurance settlements, investment operations and regulatory reporting.
- Align timelines, where practical, with India's quantum-safe ecosystem roadmap, focusing on long-lived data and digital signatures.
- Pilot the NIST-standardised post-quantum algorithm families directly — the lattice-based ML-KEM (Kyber) for key exchange and ML-DSA (Dilithium) for digital signatures, with the hash-based SLH-DSA (SPHINCS+) as a conservative fallback — rather than a generic 'post-quantum cryptography' pilot, so outputs are directly comparable with the algorithm choices insurers, reinsurers and cloud vendors are likely to be asked to support globally.

Catastrophe and Climate-Analytics Pilots

- Use AI, quantum or quantum-inspired methods to generate richer, more granular scenario sets for ORSA, stress testing and capital planning.
- Prioritise agriculture, property and health portfolios, where climate and catastrophe risk is structurally important.

Reinsurance and Capital-Optimisation Pilots

- Apply quantum-inspired solvers to treaty design and capital allocation.
- Benchmark against current treaty structures and solvency metrics, and explicitly assess model-risk and governance implications.

Operational Design Features

- **Scope and safeguards:** clear limits on customer exposure, product volumes and financial impact per pilot, with compulsory opt-in and disclosure where customers are involved.
- **Data and security:** minimum standards on data quality, encryption, access controls, logging, monitoring and incident response, with additional requirements for pilots that touch core cryptography. Sandbox designs should be able to demonstrate the ability to identify, contain and escalate qualifying cyber incidents within applicable regulatory reporting timelines, including the six-hour window under CERT-In's 2022 Directions.
- **Reporting and transparency:** standardised templates for firms to report objectives, methodology, metrics and outcomes, with regular supervisory touchpoints during each pilot.

Potential pathways following a pilot could include wider application, further testing or refinement, depending on the evidence and outcomes. Pilots that do not progress further may still provide useful insights into model risk, governance, consumer outcomes and operational resilience, contributing to future research, learning and capacity building.

6.3 A Two-Step Quantum-Ready Framework (Now–2029)

The table below sets out a possible two-step approach for the sector between now and 2029.

Step 1 focuses on actions that most insurers can reasonably begin now, largely regardless of how quantum timelines evolve : awareness, mapping, sandbox participation and crypto-agility groundwork.

Step 2 involves more deeply embedding these considerations into governance and disclosure, which for many insurers will depend on how the technology, the business case and the regulatory landscape develop over the period.

Step	Focus	Illustrative Actions (Now–2029)
1	**Diagnose, pilot and build crypto-agility — actions that can reasonably begin now**	**Map** long-lived data, cryptographic assets and dependencies, identifying where vulnerable algorithms such as RSA and ECC remain in use. Align this with existing DPDP and CERT-In data and asset visibility requirements. **Prioritise** systems using Mosca's lens (X + Y vs Q), while recognising uncertainty around the timing of quantum risk. **Test** AI + quantum use cases through supervised sandboxes, including fraud, PQC, catastrophe modelling and reinsurance optimisation. **Build crypto-agility** into keys, certificates, APIs and data protection, and incorporate quantum-readiness into technology procurement, outsourcing and contract renewals. **Review critical vendor contracts** for the ability to update cryptographic standards, require security upgrades and allocate responsibility for failures. Where migration is lengthy, consider hybrid approaches as an interim measure.

2	**Explore embedding governance and disclosure — actions likely to depend on maturity and business case**	**Assess** quantum-era scenarios, including 'harvest now, decrypt later' and future signature forgery, through ORSA, stress testing and recovery planning where relevant. **Report** cryptographic exposure, PQC migration and quantum readiness through existing board risk and cyber-resilience reporting. **Embed** AI and quantum considerations progressively into risk appetite, model governance, product oversight, outsourcing and cyber frameworks. **Align** readiness milestones, where relevant, with the National Quantum Mission and India's quantum-safe roadmap, supported by simple internal measures of progress.

Table 5: An illustrative two-step, quantum-ready framework for Indian insurers and reinsurers, now to 2029.

RSA — Rivest–Shamir–Adleman, a widely used public-key cryptosystem understood to be vulnerable to large-scale quantum attack.

ECC — Elliptic Curve Cryptography, a family of public-key schemes based on elliptic curves, also understood to be vulnerable to quantum attack.

7 Quantum-Ready Insurance: Institutional Perspectives

7.1 A Policyholder-First Lens on AI and Quantum

IRDAI's regulatory mandate for policyholder protection, prudential oversight and the orderly development of the insurance sector provides the broader context within which emerging technology considerations may be viewed. As AI becomes more deeply embedded across insurance, and quantum technologies continue to develop, questions relating to data integrity, cyber resilience, solvency and long-term policyholder protection may become increasingly relevant to the regulatory landscape.

Many of these considerations can be examined through existing frameworks and supervisory mechanisms, including enterprise risk management, ORSA, cyber resilience, governance and risk oversight.

The areas set out below are therefore presented as considerations for wider industry and policy dialogue, informed by developments in India and internationally.

Theme	A Possible Area for Continued Dialogue
Mosca's theorem as one lens among several	Suggestion could be consider inviting major insurers and reinsurers, on a voluntary basis, to share how they think about X, Y and Q for their most long-tailed portfolios and critical systems, as one possible input into ORSA and supervisory dialogue — alongside the many other lenses already used.
Quantum-related risk in solvency oversight	Continued industry-regulator dialogue could explore whether, and how, quantum-related cyber and integrity scenarios might over time find a place within ORSA, stress testing and internal-model-style approaches, particularly for long-tail lines, as both understanding and the underlying technology mature.
Alignment with national timelines	Over time, there may be value in considering greater alignment between IRDAI's cyber security, operational resilience and outsourcing frameworks and the phased milestones of DST's National Quantum Mission quantum-safe roadmap, supporting consistency with the wider BFSI transition. Where relevant, this could also consider the interaction with DPDP obligations and CERT-In requirements, enabling data protection, cyber-incident response and quantum-safe preparedness to be viewed through a more integrated resilience lens.
Continuing to build on the sandbox programme	Continuing to expand IRDAI's existing sandbox programme to accommodate AI and quantum pilots (reinsurance optimisation, catastrophe analytics, PQC implementation) could offer a supervised route for testing these ideas, with outputs feeding into sector-wide guidance and templates over time, entirely at IRDAI's discretion and pace.

Table 6: Possible areas for continued IRDAI–industry dialogue on AI and quantum readiness — offered as discussion points.

7.2 NIA and Academia: Building National Capability

The National Insurance Academy and academic partners have an important role to play in building the long-term human capital that quantum readiness will depend on.

Priority areas that NIA and academic partners may wish to explore include:

- Developing executive and professional programmes on AI and quantum in insurance, post-quantum cryptography, long-tail risk and solvency implications — for boards, actuaries, risk officers and CISOs.
- Producing Indian case studies from sandbox pilots in reinsurance optimisation, catastrophe analytics and PQC implementation, to build an indigenous evidence base over time.
- Convening multi-stakeholder dialogues bringing together IRDAI, National Quantum Mission stakeholders, insurers, reinsurers, technology firms and academics around AI and quantum governance for policyholder protection.
- Integrating quantum-risk and quantum-safe literacy into actuarial, underwriting and risk curricula for professionals entering the Indian insurance market.

8 Conclusion: AI + Quantum for Bharat as a Test of Trust

Artificial intelligence and quantum technology are developing on different timelines, but both have implications for the future of insurance. AI is already influencing underwriting, pricing, claims, fraud detection and customer engagement. Quantum computing remains at an earlier stage, with potential applications in areas such as risk modelling, optimisation and reinsurance still being explored.

For insurers and reinsurers, this creates two distinct but related considerations. Quantum Advantage is about where new computational approaches may, over time, improve the way complex risks are modelled, priced and managed. Quantum Readiness is about resilience: whether the data, systems, cryptography and digital trust underpinning insurance can remain secure and reliable over the long periods for which insurance obligations endure.

This distinction is particularly relevant for India. Long-duration policies, claims records, health information, reinsurance arrangements and digital signatures may need to remain protected for decades. At the same time, India is building domestic capability through the National Quantum Mission and developing a phased approach to quantum-safe infrastructure through the Department of Science & Technology. International developments in post-quantum standards and migration planning point in a similar direction: preparedness is increasingly being approached as a multi-year process rather than a response to a single future event. This is consistent with the paper's broader treatment of quantum readiness as a question of the longevity of data and the time required to migrate systems, rather than a prediction of when quantum-enabled attacks may become practical.

For the insurance sector, this need not mean creating a separate quantum programme or attempting to predict precisely when 'Q-Day' might arrive. A practical starting point is to understand long-lived data and cryptographic dependencies, build relevant capability and crypto-agility, and use pilots and sandboxes where there is a credible business or resilience case. Existing mechanisms such as enterprise risk management, ORSA, stress testing, cyber resilience, data governance and board oversight provide a practical foundation for taking these considerations forward.

India's AI, data-protection, cybersecurity and quantum-safe agendas rest on distinct legal, regulatory and policy foundations. They should not be conflated, but there is value in understanding where they intersect, particularly around the protection and integrity of data and the resilience of the systems on which insurers and policyholders increasingly depend. Existing ERM, ORSA and sandbox mechanisms provide avenues for considering these questions without necessarily creating new governance structures.

The direction of this agenda will continue to evolve, shaped by policymakers and regulators and informed by the experience of insurers, reinsurers, industry, academia and the wider research community. Greater clarity will emerge as technology develops, standards mature and practical experience grows. Building awareness and capability progressively can help the sector assess these developments and respond in a measured and proportionate way.

Insurance is ultimately a promise made across time. As AI becomes more deeply embedded and quantum technologies develop, the test is not simply which technologies the sector adopts, but whether the data, systems and digital trust supporting those promises remain secure, resilient and governable over their full life. For India's insurance ecosystem, preparing for that future is as much a question of trust and resilience as it is of technology.

9 Glossary

AI (Artificial Intelligence)

A broad set of computational techniques that allow systems to identify patterns, make predictions, automate decisions and generate content or insights from data.

Amaravati Quantum Valley

A flagship quantum-technology hub in Amaravati, Andhra Pradesh, associated with the National Quantum Mission and intended to support quantum computing, communication and application development in India.

CERT-In (Indian Computer Emergency Response Team)

India's national nodal agency for cybersecurity incident response under the Information Technology Act, 2000. Its Directions of 28 April 2022 require specified cyber incidents, including data breaches and data leaks, to be reported within six hours of detection; its 25 May 2026 Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation sets out complementary guidance on continuous exposure management, AI governance, data-centric security and third-party risk.

CSCRF (Cyber Security and Cyber Resilience Framework)

A cyber-governance and resilience framework issued by the Securities and Exchange Board of India (SEBI).

Crypto-agility

The ability of systems, applications and infrastructure to change cryptographic algorithms, parameters or implementations without major operational disruption.

Data Fiduciary

Under the DPDP Act, 2023, any person (including an insurer or reinsurer) who alone or with others determines the purpose and means of processing personal data, and who bears the associated compliance duties — purpose limitation, storage limitation, security safeguards and breach notification.

Data Protection Board of India

The adjudicatory body established under the DPDP Act, 2023 to receive personal-data-breach notifications, enforce compliance and impose penalties for non-compliance with the Act and the DPDP Rules, 2025.

Department of Science and Technology (DST)

A department of the Government of India responsible for science and technology policy, and a key sponsor of India's quantum-safe ecosystem roadmap.

DPDP Act, 2023 (Digital Personal Data Protection Act, 2023)

India's principal personal-data-protection statute (No. 22 of 2023), setting out data-fiduciary obligations including purpose limitation, storage limitation, reasonable security safeguards and breach notification — directly relevant to the long-lived personal data insurers hold.

DPDP Rules, 2025 (Digital Personal Data Protection Rules, 2025)

Rules notified by MeitY under the DPDP Act, 2023 that operationalise the Act, including prescribed timelines for notifying the Data Protection Board of India and affected individuals of a personal-data breach.

Harvest now, decrypt later

An attack model in which adversaries steal encrypted data today and store it until future quantum computational advances make it decryptable.

IRDAI (Insurance Regulatory and Development Authority of India)

India's insurance regulator, responsible for the orderly growth of the insurance sector and protection of policyholders' interests.

MeitY (Ministry of Electronics and Information Technology)

The Government of India ministry responsible for electronics, information technology, cyber-related policy and digital initiatives, including quantum-safe innovation.

Mosca's Theorem

A governance framework for thinking about quantum-related risk: if the time data must stay secure (X) plus the time needed for cryptographic migration (Y) is likely to exceed the time before quantum-enabled attacks become practical (Q), earlier preparation may be warranted. Q itself cannot be estimated with precision, so the framework is best used directionally rather than as a countdown.

National Quantum Mission (NQM)

India's national mission to build sovereign capability in quantum computing, communication, sensing and materials.

ORSA (Own Risk and Solvency Assessment)

An insurer's internal process for assessing its overall risk profile, solvency needs and resilience under current and projected future scenarios.

Post-Quantum Cryptography (PQC)

Cryptographic algorithms designed to remain secure against both classical and quantum-enabled attacks — intended successors to current public-key cryptography.

Q-Day

An informal shorthand for the point at which quantum-enabled attacks might become able to break widely deployed cryptographic systems at meaningful scale. Estimates of its timing vary considerably across credible sources, and this paper uses the term descriptively, to aid discussion, rather than as a prediction of when that point will arrive.

Quantum annealing

A quantum or quantum-inspired optimisation technique suited to certain constrained combinatorial problems, including portfolio and treaty optimisation.

Quantum Key Distribution (QKD)

A quantum communication technique for distributing cryptographic keys with security properties derived from the laws of physics.

Trust now, forge later

The future integrity risk that records, digital signatures or certificate chains that appear trustworthy today may become forgeable or legally contestable once the cryptography protecting them is compromised by a quantum-enabled attack.

10 References and Footnotes

Indian Primary Regulatory and Government Sources

- Government of India, National Quantum Mission: Mission Document and Press Releases, Ministry of Science and Technology, 2024–2026; and Government of India, 'India's First Quantum Computer Launched at Amaravati Quantum Valley,' Press Release, 14 April 2026.
- Department of Science and Technology, Implementation of Quantum Safe Ecosystem in India: Report of the Task Force, New Delhi: Government of India, February 2026.
- Government of India, Digital Personal Data Protection Act, 2023 (No. 22 of 2023), India Code, https://www.indiacode.nic.in/handle/123456789/22037
- Ministry of Electronics and Information Technology (MeitY), Digital Personal Data Protection Act, 2023 (official text), February 2024, https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023.pdf
- Ministry of Electronics and Information Technology (MeitY), Digital Personal Data Protection Rules, 2025, https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa
- Indian Computer Emergency Response Team (CERT-In), Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, 28 April 2022, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
- Indian Computer Emergency Response Team (CERT-In), Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure, 25 May 2026, https://www.cert-in.org.in/PDF/Blueprint_for_Defending_against_AI_Assisted_Exploitataion.pdf
- Insurance Regulatory and Development Authority of India (IRDAI), Information and Cyber Security Guidelines (2023, revised April 2026).
- Reserve Bank of India, constitution of the Q-SAFE Expert Committee on quantum risk to the financial sector, May 2026.
- Securities and Exchange Board of India (SEBI), Cyber Security and Cyber Resilience Framework (CSCRF), 2024.
- Government of India, Ministry of Finance, Department of Financial Services, "DFS Secretary Highlights India's Insurance Growth at IFSCA–IRDAI–GIFT City Global Reinsurance Summit," Press Information Bureau, 19 January 2026.
- Government of India, Ministry of Health and Family Welfare, "Update on Progress of AB-PMJAY and ABDM," Press Information Bureau, 17 March 2026.
- Insurance Regulatory and Development Authority of India (IRDAI), Annual Report 2024–25 (Hyderabad: IRDAI, 2025).
- Press Information Bureau, Government of India, "Insurance for All: Expanding Coverage, Strengthening Social Security," April 2026.

International Regulators and Standards Bodies

- National Institute of Standards and Technology (NIST), NIST IR 8547 (Initial Public Draft), Transition to Post-Quantum Cryptography Standards, 2024, setting out the proposed timeline to deprecate RSA and elliptic-curve cryptography after 2030 and disallow their use after 2035.
- Bank for International Settlements, Quantum Computing and the Financial System: Opportunities and Risks, BIS Papers No. 149 (Basel: BIS, 2024).
- European Insurance and Occupational Pensions Authority (EIOPA), Report on the Digitalisation of the European Insurance Sector, 30 April 2024, https://www.eiopa.europa.eu/document/download/6ca9e171-42b9-44d7-a2e6-beaf0134ecb8_en?filename=Report+on+the+digitalisation+of+the+european+insurance+sector.pdf
- European Insurance and Occupational Pensions Authority (EIOPA), Methodological Principles of Insurance Stress Testing — Cyber Component, 11 July 2023, https://www.eiopa.europa.eu/publications/methodological-principles-insurance-stress-testing-cyber-component_en

- European Insurance and Occupational Pensions Authority (EIOPA), 'EIOPA Insurance Risk Dashboard Shows Broadly Stable Risk Environment Even as Cyber and Geopolitical Risk Intensify,' 30 July 2026, https://www.eiopa.europa.eu/eiopa-insurance-risk-dashboard-shows-broadly-stable-risk-environment-even-cyber-and-geopolitical-2026-07-30_en
- Garante per la protezione dei dati personali (Italian Data Protection Authority), 'Security Preparedness Under the GDPR: The (Possible) PQC Impact,' presented via ENISA, 8 December 2025, https://www.enisa.europa.eu/media/56883
- National Institute of Standards and Technology (NIST), 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards' (FIPS 203, FIPS 204 and FIPS 205), 13 August 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- UK National Cyber Security Centre (NCSC), 'Timelines for Migration to Post-Quantum Cryptography' (guidance, 2025), https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
- European Telecommunications Standards Institute (ETSI), TS 104 015, 'Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies,' 25 March 2025, https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption/
- European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- European Insurance and Occupational Pensions Authority (EIOPA), Cyber Risk for Insurers — Challenges and Opportunities, 1 September 2019, https://www.eiopa.europa.eu/publications/cyber-risk-insurers-challenges-and-opportunities_en
- European Union, Regulation (EU) 2022/2554 (Digital Operational Resilience Act), 14 December 2022, https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- European Union, Directive 2009/138/EC (Solvency II), 25 November 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0138
- European Commission, Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 11 April 2024, https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
- European Commission and EU Member States, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 23 June 2025, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
- G7 Cyber Expert Group, G7 CEG Quantum Roadmap, January 2026, https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf
- Monetary Authority of Singapore (MAS), remarks by Chia Der Jiun, Managing Director, at the MAS Annual Report 2025/2026 Media Conference, 28 July 2026, republished by the Bank for International Settlements, https://www.bis.org/review/r260813l.htm

Academic and Foundational Sources

- Michele Mosca, 'Cybersecurity in an Era with Quantum Computers,' in Quantum Information Science and Its Contributions to Mathematics, ed. S. Severini (Providence, RI: American Mathematical Society, 2010).

Industry and Professional Bodies

- Gesamtverband der Deutschen Versicherungswirtschaft (GDV — German Insurance Association), 'Quantum Computing — Implications for the Insurance Sector and Its Customers,' https://www.gdv.de/resource/blob/189418/9772c1c55c77e72b8ceb130e7ae55eb8/quantum-computing-implications-for-the-insurance-sector-and-its-customers-data.pdf
- Lloyd's City Risk Index 2015–2025 — Executive Summary, produced with the Cambridge Centre for Risk Studies, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloydscityriskindex-execsummary.pdf
- World Economic Forum, 'Optimization of Reinsurance Contracts,' in quantum and financial-services case-study materials (World Economic Forum, 2023).

- Insurance Thought Leadership, 'Ransomware Trends 2026: What Cyber Insurers Need to Know,' https://www.insurancethoughtleadership.com/cyber/ransomware-trends-2026-cyber-insurers
- Accenture, 'What Quantum Computing Means for Insurance,' Accenture Insurance Blog, 25 July 2022.
- Databricks, 'Navigating the Impact of AI in Insurance: Opportunities and Challenges,' industry brief, 2025.
- Kevin Russell, Kweilin Ellingrud, Sebastian Kohls, Tanguy Catlin, and Suhayl Chettih, 'The Strategic New Arenas Reshaping Insurance,' McKinsey & Company, 15 September 2026, https://www.mckinsey.com/industries/financial-services/our-insights/the-strategic-new-arenas-reshaping-insurance.
- Jason Ralph, Johannes-Tobias Lorenz, Nick Milinkovich, Sid Kamath, Tanguy Catlin, and Gabriella Meijer, "How AI Will Reshape the Economics of Insurance: A CEO's Guide to Strategy," McKinsey & Company, July 23, 2026, McKinsey & Company.
- Arjun Ganguly, Sara Codella, Nadine Moore, and Daniel Yang, "The AI-First Property and Casualty Insurer," Boston Consulting Group, March 30, 2026, Boston Consulting Group.
- Cullen Breithaupt, Arjun Ganguly, Drew Ingalls, and Rebecca Waddell, "The AI-First Life Insurance Company," Boston Consulting Group, January 22, 2026, Boston Consulting Group.
- Muhsin Tamturk, Eran Ginossar, Marco Carenzo, and Claude Perret, "Motor Insurance Data Analysis by Quantum Machine Learning," *Discover Quantum Science* 2, article 3 (2026), published February 10, 2026, Springer Nature. https://doi.org/10.1007/s44464-026-00007-x

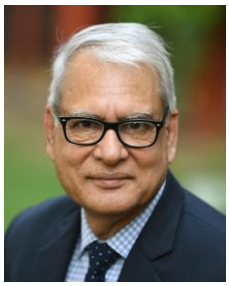
Legal and Consulting Commentary

- Karishma Paroha, Hogan Lovells Cadwalader, 'Emerging Risks in 2026: Preparing for the Legal and Regulatory Implications of Quantum,' 20 May 2026, https://www.hlc.com/en/publications/emerging-risks-in-2026-preparing-for-the-legal-and-regulatory-implications-of-quantum
- Herbert Smith Freehills Kramer, 'Teetering on the Brink of Quantum Utility — Not If, But When,' FSR Outlook 2025, https://www.hsfkramer.com/insights/reports/2025/fsr-outlook-2025/teetering-on-the-brink-of-quantum-utility-not-if-but-when

Commercial Media

- Financial Express CIO, 'How AI Is Fueling Insurance Revolution, Paving the Way for Viksit Bharat 2047,' The Financial Express, 23 December 2025.
- World Finance Informs, 'Inside Quantum Encryption's Impact on Insurance Security,' https://www.worldfinanceinforms.com/trends/inside-quantum-encryptions-impact-on-insurance-security/

11 About the Authors



Arun Agarwal

Author; Professor of Practice, Rizvi Institute of Management Studies and Research, and recipient of the Lifetime Achievement Award at the 24th Asia Insurance Industry Awards, 2020, Singapore

Arun Agarwal is a veteran of over 46 years in the Indian and global insurance industry, with a career spanning leadership, market-building and regulatory engagement. He played a founding role in three major insurance and reinsurance start-ups in India: as the first employee of AIG in India and a founding member of Tata AIG General Insurance; as founding Managing Director and CEO of Chola MS General Insurance, the joint venture between the Murugappa Group and Mitsui Sumitomo; and as Lloyd's Chief Executive for India, where he helped secure legislative changes to permit onshore reinsurance branches, shape the regulatory framework, and operationalise Lloyd's in India. He has also served as an Independent Director on the Board of Kotak Mahindra General Insurance Company and chaired its Audit Committee.

Anita Nandi

Co-Founder and Policy Director, Kquanta Research LLP

Anita Nandi works across financial services, emerging technology and public policy, helping boards, regulators and institutions think through the artificial intelligence and quantum era. At Kquanta Research, she leads policy strategy, thought leadership and executive education, translating complex AI and quantum developments into practical insight for financial institutions, while working to strengthen institutional and talent readiness across India's financial sector. She previously served as India Head and Chief Representative for the City of London Corporation, leading UK–India financial-sector engagement across capital markets, fintech and sustainable finance. Earlier in her career, she held senior roles with American Express Europe in Amsterdam and London.

12 About Kquanta Research

Kquanta Research is an independent research and advisory firm focused on finance, emerging technology and sustainability. We translate complex technological developments into strategic insight for boards, financial institutions, regulators and policymakers, with a focus on governance, resilience and future readiness.

Our work brings together industry, academia, policymakers and technology experts through independent research, executive education, strategic advisory and industry dialogue. The Kquantalyst Thought Leadership Forum is our convening platform for advancing informed discussion on the technological and structural shifts shaping the future of finance.

'New Frontiers: AI + Quantum Technology — Future-Proofing Insurance for Bharat' is the first white paper published by Kquanta Research for the insurance sector, and the beginning of a wider research series. It reflects our commitment to examining the opportunities, emerging risks and policy implications of technological change through an India-focused, globally informed lens — beginning with insurance and reinsurance and extending across the wider financial services landscape.

Kquanta Research LLP

Contact: Shraddha Joshi | Email: shraddha.joshi@kquantaresearch.com

Corporate Office: One World Centre, 9th Floor, Elphinstone, Lower Parel, Mumbai 400013, Maharashtra, India

Website: www.kquantaresearch.com