QUANTNEXUS • QUANTZEN™

QuantNexus Cybersecurity White Paper
QN CSWP 01

Post-Quantum Readiness for Organizations

A Non-Technical Guide for Enterprises & Institutions



Ashish Janghel
Adrian Hernandez
Nitish Naik
QuantZen Platform & Security Architecture
QuantNexus Technology Private Limited

Bengaluru, India
Indian Patent Application No. 202641078837 (Pending)
ISO 9001:2015 Certified (Certificate No. E20260852167)

This publication is available on the QuantNexus website:
https://www.quantzenpqc.com

November 2026

Abstract

This white paper is written in clear, non-technical language to help business leaders, banks, technology companies, and hardware manufacturers prepare for post-quantum cybersecurity transitions. Modern digital operations depend on mathematical encryption locks across customer applications, payment gateways, cloud storage, and connected devices. Advances in quantum computing and binding international mandates between 2026 and 2030 require organizations to map where encryption resides and plan safe, non-disruptive upgrades. This document introduces practical readiness concepts alongside the QuantZen™ sovereign security platform without requiring deep cryptography expertise.

Keywords

cryptographic readiness; crypto-agility; post-quantum security; digital lock inventory; banking resilience; connected device lifecycle; QuantZen; QuantNexus.

Audience

This publication serves executives, board risk committees, compliance officers, procurement teams, operations leads, and security advisors at any organization, whether running four local office servers, a multi-branch bank, a software enterprise, or connected hardware product lines. Because organizations differ widely in scale and regulation, the readiness principles presented here adapt cleanly across sectors.

Credentials and Governance

QuantNexus Technology Private Limited operates in Bengaluru, India (CIN: U63999KA2026PTC222762) under an independently audited ISO 9001:2015 Quality Management System (Certificate No. E20260852167) scoped to cybersecurity software kits, vulnerability assessment, quality assurance, deployment, and technical support, alongside DPIIT startup recognition, ISO 27001 aligned practices, and Indian Patent Application No. 202641078837.

Relationship to Global Standards

Guidance in this paper aligns with published roadmaps from the Reserve Bank of India (RBI Q-SAFE), India Digital Personal Data Protection (DPDP) Rules, the National Institute of Standards and Technology (NIST), the European Cyber Resilience Act (EU CRA), and national quantum readiness initiatives.

Table of Contents

1. Introduction 4
1.1. Foundational Goals of Digital Trust 4
1.2. Immediate Practical Checklist for Any Company 5
1.3. Why Current Digital Locks Are Expiring 5
2. Global Regulatory and Market Context 6
3. Understanding Your Organization's Digital Lock Footprint 7
4. Elements of Transition Risk and Traditional Blind Spots 8
5. The QuantZen™ Three-Step Readiness Framework 9
5.1. Stage One: Complete Digital Lock Visibility 10
5.2. Stage Two: Safe Compatibility Checks and Rehearsal 11
5.3. Stage Three: Tamper-Proof Audit Evidence 11
6. Securing Smart Devices and Long-Life Hardware 12
7. Privacy, Data Sovereignty, and Offline Operations 13
8. Industry Use Cases, Adoption Path, and Leadership 14
9. Transparency Notice and References 15

List of Tables

Table 1. Global Regulatory and Standards Milestones (2026 to 2031) 6
Table 2. Getting Started with a Basic Digital Lock Inventory 7
Table 3. Key Elements of Cryptographic Transition Risk 8
Table 4. Executive Priority Mapping for Identified Findings 10
Table 5. Connected Device and Hardware Lifecycle Stages 12
Table 6. Flexible Enterprise Deployment Models 13
Table 7. Zero-Risk Four-Step Organizational Onboarding 14

List of Figures

Fig. 1. Foundational Triad of Organizational Digital Trust 4
Fig. 2. Projected Global Post-Quantum Security Shift (2025 to 2033) 6
Fig. 3. Typical Business Environment and Encryption Touchpoints 7
Fig. 4. QuantZen™ Three-Step Readiness Workflow 9

1. Introduction

Digital operations sit at the center of almost every modern enterprise, from cooperative banks and payment processors to software firms, hospitals, and manufacturers. Every online login, customer transaction, vendor update, and cloud backup relies quietly on mathematical encryption locks to ensure information stays confidential and authentic.

As businesses adopt cloud infrastructure, digital payments, and connected devices, cryptographic protection must be managed as an ongoing business risk alongside financial, legal, and operational governance. A sudden failure in digital trust or an inability to upgrade outdated encryption can interrupt customer payments, expose sensitive records, or stall compliance approvals. Establishing clear visibility early allows an organization to modernize smoothly without replacing core systems.

1.1. Foundational Goals of Digital Trust

Three foundational goals underpin cryptographic security across any enterprise environment: confidentiality, integrity, and continuous availability of critical systems.[1]

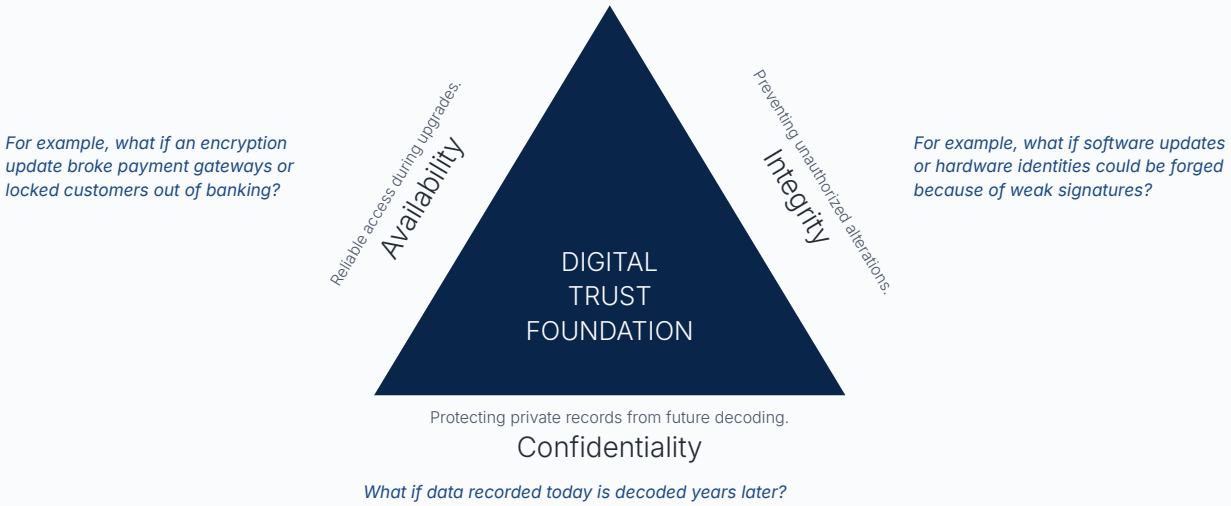


Fig. 1. Foundational Triad of Organizational Digital Trust

[1] Regulated infrastructure sectors often add safety and non-repudiation alongside these three foundational goals.

1.2. Immediate Practical Checklist for Any Company

Business leaders do not need to wait for full system replacements before taking smart action. Starting with clear organizational habits significantly reduces exposure across software and hardware assets:

- Identify your most sensitive business records that must stay private for five to fifteen years.
- Inventory every customer portal, payment gateway, cloud service, and third-party vendor package.
- Ask software and hardware suppliers when their products will support modern post-quantum standards.
- Separate sensitive master keys from everyday application configuration files by moving keys into secure vaults.
- Test encryption changes in an isolated rehearsal environment before touching live customer operations.
- Track legal and sector deadlines affecting banking, privacy protection, and connected product exports.
- Build repeatable compliance reporting rather than relying on one-time annual spreadsheet audits.

1.3. Why Current Digital Locks Are Expiring

For three decades, global digital security has relied primarily on classical public-key locks (widely known as RSA and ECC). These locks depend on math puzzles that take standard computers thousands of years to break. However, two structural shifts now challenge these legacy foundations:

- Future Quantum Decryption Risk: Emerging quantum machines solve those specific classical math puzzles vastly faster, meaning legacy locks will no longer protect long-lived data or device identities indefinitely.
- "Harvest Now, Decrypt Later": Hostile actors do not wait for tomorrow's computers; they capture and store encrypted financial, corporate, and health data today expecting to unlock those archives years from now.
- Crypto-Agility Readiness: Rather than rushing an emergency overhaul later, crypto-agility enables companies to locate every digital lock now and swap locks safely as international standards evolve.

2. Global Regulatory and Market Context

Governments, central banks, and international cybersecurity agencies have moved post-quantum preparation from theoretical research into concrete compliance calendars spanning 2026 through 2031.

Table 1. Global Regulatory and Standards Milestones (2026 to 2031)

Jurisdiction / Body	Target Window	Practical Mandate for Organizations
Reserve Bank of India (Q-SAFE)	May to Sept 2026	Evaluates financial ecosystem quantum readiness and encourages quantum-proofing payment systems.
India DPDP Rules, 2025	May 13, 2027	Mandates reasonable encryption and security safeguards, with statutory failure penalties up to ₹250 Crore.
National Quantum Mission (India)	2024 to 2031	₹6,003.65 Crore national initiative advancing sovereign quantum-safe infrastructure across sectors.
European Cyber Resilience Act	Dec 11, 2027	Requires software/security inventories and updateable lifecycles for digital products sold in Europe.
United States Federal Standards	2027 to 2030	Deprecates classical RSA and ECC locks after 2030 and requires critical procurement transitions early.
UAE, France & UK Warnings	2027 to 2029	National policies restrict non-resistant security products; Google and IBM emphasize 2029 readiness urgency.

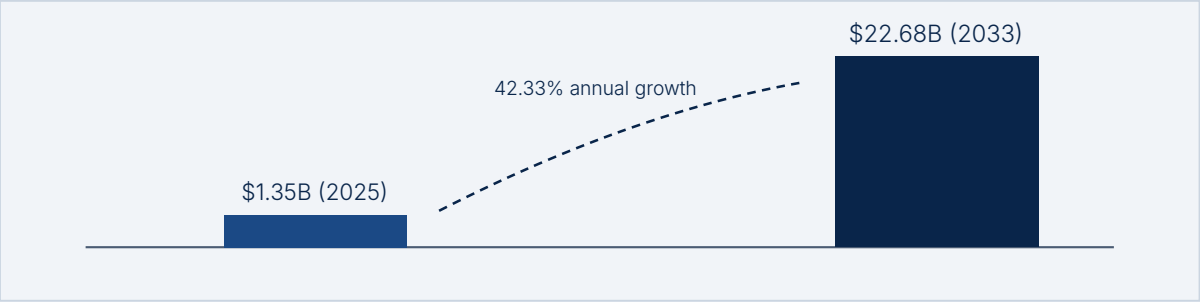


Fig. 2. Projected Global Post-Quantum Security Market Expansion (Grand View Research)

3. Understanding Your Organization's Digital Lock Footprint

Before selecting new security software or negotiating vendor upgrades, a company must understand where digital locks exist across its applications, external providers, and computing devices. Creating a basic inventory clarifies which systems store sensitive data, how external partners connect, and where older protections live.

Table 2. Getting Started with a Basic Digital Lock Inventory

Software, Device or Service Name	System Owner	Data Sensitivity Level	Deployment Location	Business Impact if Exposed	Key Vault Protected?	Upgrade Tested?

A straightforward environment diagram helps leadership see how every business layer connects. Fig. 3 illustrates typical encryption touchpoints across internal devices, enterprise networks, banking links, and cloud services.

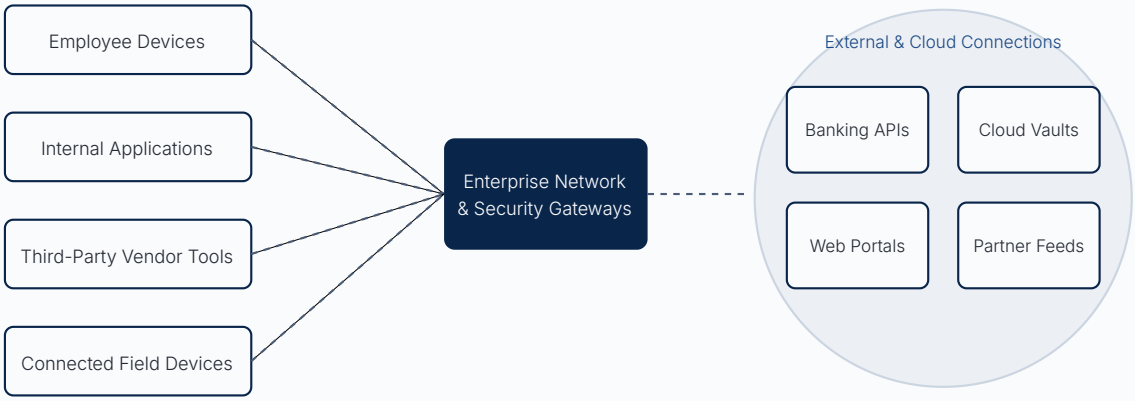


Fig. 3. Typical Business Environment and Encryption Touchpoints

4. Elements of Transition Risk and Traditional Blind Spots

Upgrading digital locks across an active business differs from installing ordinary software patches. Even organizations with dedicated security teams run into four practical obstacles when relying only on spreadsheets or periodic external scans. Transition readiness is best evaluated through four specific risk elements shown in Table 3.

Table 3. Key Elements of Cryptographic Transition Risk

Hidden Vendor Dependencies	An external component risk occurs when commercial apps or acquired tools contain older encryption hidden inside compiled packages. Because buyers rarely have access to vendor source files, surface scanners miss these dependencies entirely until a compliance review stalls.
Size and Compatibility Limits	Modern quantum-resistant keys and signatures require noticeably larger digital space than older protections. Rigid legacy modules, memory slots, or communication links designed around tiny limits can fail or drop messages unless checked in advance.
Live Policy Divergence	Operational drift occurs when written security documents state that modern protections are active while older test servers, forgotten cloud links, or live partner connections quietly continue accepting outdated protocols.
Key Storage and Randomness	Key custody risk arises when master digital secrets are left inside everyday configuration files or generated using predictable shortcuts rather than secure hardware vaults, weakening even upgraded encryption standards.

4.1. Why Traditional Tools Cannot Solve These Elements Alone

Annual vulnerability testing examines surface openings at one point in time, and certificate managers track only public web expiry dates. Neither tool traces hidden locks inside internal systems, predicts upgrade compatibility crashes, or supplies continuous audit evidence across updates.

5. The QuantZen™ Three-Step Readiness Framework

QuantZen™, developed by QuantNexus Technology Private Limited, unifies discovery, safe upgrade planning, and compliance proof inside one platform. Organizations do not have to discard core banking software, payment switches, or cloud applications to prepare for new standards.

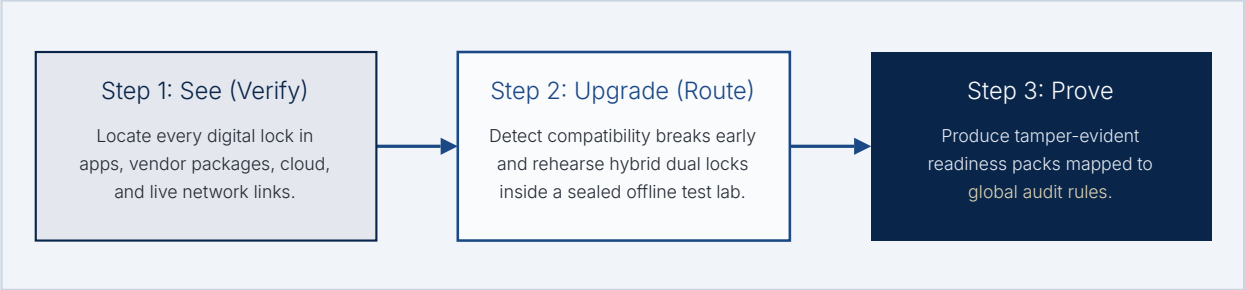


Fig. 4. QuantZen™ Three-Step Readiness Workflow

Through this unified structure, organizations gain shared clarity across three architectural layers: customer applications and APIs, cloud and internal server infrastructure, and long-life connected devices or hardware foundations. Every decision remains transparent and human-approved.

5.1. Stage One: Complete Digital Lock Visibility

Effective transition planning starts by replacing guesswork with an exact, searchable inventory. QuantZen™ inspects internal software code across major programming languages as well as finished third-party software packages, allowing teams to discover outdated locks even when vendor source code is unavailable.

At the infrastructure layer, QuantZen™ connects to cloud accounts strictly in read-only configuration mode (never reading customer data or decrypting secrets), while optionally observing live server handshakes inside the local environment to confirm real production security matches written policies.

Table 4. Executive Priority Mapping for Identified Findings

Finding Type	Plain-English Meaning	Recommended Business Action
Legacy Public Locks	Customer gateways or payment APIs still relying solely on older public locks.	Schedule dual-lock hybrid transition ahead of regulatory dates.
Third-Party Package Risk	Purchased libraries using outdated signature checks internally.	Confirm vendor roadmap or shield via controlled gateway routing.
Exposed Master Keys	Keys or secrets stored inside everyday files instead of dedicated vaults.	Immediate move into secure key management hardware.
Predictable Randomness	Shortcuts used during key creation that reduce mathematical strength.	Replace with verified system random number generators.
Undersized Memory Limits	Legacy software parts unable to hold larger modern security keys.	Expand buffer capacity cleanly during routine release cycles.

5.2. Stage Two: Safe Compatibility Checks and Rehearsal

Executives understandably worry that security changes might interrupt mission-critical banking or customer portals. QuantZen™ minimizes operational downtime through three protective steps before any production deployment:

- Pre-Flight Compatibility Check: QuantZen™ predicts which legacy systems can accept larger next-generation locks immediately and which ones need simple size adjustments first.
- Isolated Offline Rehearsal: Proposed upgrades run inside an isolated local test room alongside your functional software tests. Any change that breaks an existing test is halted automatically.
- Gradual Dual-Lock Transition: Hybrid configurations pair proven existing protections with new quantum-safe standards side by side, keeping external partner connections working smoothly while raising resilience immediately.

5.3. Stage Three: Tamper-Proof Audit Evidence

Compliance audits often stall when teams must manually gather screenshots and scattered logs weeks before inspections. QuantZen™ records every discovery scan, test rehearsal, and readiness check inside a cryptographically linked, tamper-evident trail.

Evidence exports align cleanly across 19 global and regional regulatory catalogs, helping banks, fintechs, and technology suppliers demonstrate progress to central banks, privacy authorities, and enterprise buyers while keeping realistic quantum timelines grounded in peer-reviewed engineering estimates rather than hype.

> - Clarification on Assurance: Generating readiness reports supports external audits and governance oversight, while formal regulatory certification applies to the complete organization as issued by accredited authorities.

6. Securing Smart Devices and Long-Life Hardware

While cloud services can receive weekly updates, connected medical instruments, industrial controllers, vehicles, telecom nodes, and custom silicon chips frequently remain operating in the field for 10 to 15 years. Products shipped in 2027 must remain resilient as international mandates such as the European Cyber Resilience Act take hold.

Today, QuantZen™ analyzes device software and compiled packages to spot size limits and randomness flaws early. Alongside active hardware and cryptography partner pilots, QuantNexus extends these assessments into a five-stage device and silicon readiness lifecycle summarized in Table 5.

Table 5. Connected Device and Hardware Lifecycle Stages (Built vs. Pilot Roadmap)

Lifecycle Stage	Design & Security Objective	Practical Value for Manufacturers
1. Concept Review	Identify long-term data and firmware exposure during initial product definition.	Avoids expensive redesigns late in manufacturing.
2. Trust Architecture	Define updateable key storage and hardware agility principles early.	Enables safe security updates years after field deployment.
3. Sizing Specs	Align post-quantum footprints with strict microcontroller memory and power limits.	Matches partner cryptography libraries cleanly without hardware bloat.
4. Verification	Validate algorithm behavior, link message limits, and key randomness quality.	Prevents wireless connection drops under larger signatures.
5. Market Readiness	Compile per-product-family readiness packs for regulators and enterprise buyers.	Supports smoother international certifications and export audits.

7. Privacy, Data Sovereignty, and Offline Operations

Handling proprietary business software and encryption inventories requires strict trust. Many cloud-based security providers expect companies to upload source code or grant broad external access, an approach often restricted by banking secrecy rules, national localization policies, and internal corporate governance.

QuantZen™ is built from inception to operate strictly inside the customer's chosen perimeter, with zero requirement to transmit source code, private keys, or sensitive customer records outside your organization.

Table 6. Flexible Enterprise Deployment Models

Deployment Topology	Operational Behavior	Ideal Organizational Fit
Air-Gapped On-Premises	Operates completely offline inside isolated internal data centers with zero internet access.	Cooperative banks, core banking setups, defense, and critical utilities.
Private Cloud VPC	Runs solely inside your organization's cloud account using read-only configuration visibility.	Fintechs, payment platforms, digital commerce, and healthcare SaaS.
Internal Build Pipeline	Checks new software releases and device packages quietly inside private engineering servers.	Device manufacturers, automotive suppliers, and IT integrators.

7.1. Core Privacy Boundaries Enforced by Design

- Hardware Vault Custody: Master signing keys remain untouched inside your existing hardware vaults; QuantZen™ never exports or copies private key material.
- Read-Only Cloud Posture: Infrastructure adapters inspect encryption settings without reading customer balances, personal files, or database contents.
- Protected Internal Storage: Platform credentials and telemetry queues remain encrypted at rest under strict organizational control.

8. Industry Use Cases, Adoption Path, and Leadership

Across banking, fintech, connected hardware, telecom, healthcare, and enterprise IT services, organizations share the same fundamental need: gaining rapid visibility without disrupting live operations. QuantZen™ integrates cleanly alongside internal teams, core banking providers, and consulting partners through the four-step onboarding path in Table 7.

Table 7. Zero-Risk Four-Step Organizational Onboarding

Step	Timeframe	Scope & Tangible Outcome Delivered
Step 1	Day 1	Guided sandbox demonstration using sample systems (no company files needed).
Step 2	Weeks 1 to 3	Isolated non-production pilot inside your perimeter delivering an initial visibility briefing.
Step 3	Weeks 4 to 8	Full digital lock inventory, compatibility assessment, and offline transition rehearsal.
Step 4	Ongoing	Continuous monitoring across releases and automated board and audit compliance packs.

8.1. Sector Applicability Summary

Financial institutions secure mobile banking, ATM switches, and payment gateways under RBI Q-SAFE and DPDP expectations; software enterprises accelerate customer security reviews; hardware makers prepare 10-to-15-year products ahead of European rules; and system integrators automate client migration backlogs in days rather than months.

8.2. Leadership Team

- Ashish Janghel (Founder & Lead Architect): Cryptographic security engineer and named inventor on QuantNexus's patent application, leading core software architecture and delivery.
- Adrian Hernandez (Chief Technology Officer, Hardware & Silicon, USA): Hardware and connected-device veteran guiding international OEM and semiconductor partner strategy.
- Nitish Naik (Chief Marketing Officer): Enterprise banking and commercial strategy leader driving partner channels and regulated sector adoption.

9. Transparency Notice and References

9.1. Publication Scope and Evaluation Notice

This publication is issued by QuantNexus Technology Private Limited for general educational, executive, and evaluation purposes. Capabilities described encompass QuantZen™'s production software modules alongside scoped partner-activated hardware co-design roadmaps. Adopting readiness and discovery software supports internal risk reduction and third-party inspections; formal certification of a complete enterprise environment remains governed by accredited regulators and independent auditors.

9.2. Corporate Contact Information

QuantNexus Technology Private Limited (CIN: U63999KA2026PTC222762) • HSR Layout, Bengaluru, Karnataka, India • ISO 9001:2015 Certificate No. E20260852167 • Indian Patent Application No. 202641078837 • Website: https://www.quantzenpqc.com • Email: ashish.janghel@quantzenpqc.com • Phone: +91 8147875359.

References

[1] National Institute of Standards and Technology (NIST), Cybersecurity White Paper Series & Post-Quantum Cryptography Standards (FIPS 203, FIPS 204, FIPS 205), https://csrc.nist.gov/projects/post-quantum-cryptography

[2] National Institute of Standards and Technology (NIST), NIST IR 8547: Transition to Post-Quantum Cryptography Standards, https://csrc.nist.gov

[3] Reserve Bank of India (RBI), Quantum Secure and Adaptive Financial Ecosystem (Q-SAFE) Initiative & Digital Payment Security Directives (2026).

[4] Ministry of Electronics and Information Technology (MeitY), Government of India, Digital Personal Data Protection (DPDP) Rules (2025).

[5] Department of Science & Technology, Government of India, National Quantum Mission (NQM, 2024 to 2031).

[6] European Union, Cyber Resilience Act (EU CRA) Product Security Obligations (Enforcement Dec 2027).

[7] Grand View Research, Post-Quantum Cryptography Market Size, Share & Trends Analysis Report (2026 to 2033).

[8] QuantNexus Technology Private Limited, ISO 9001:2015 Certificate No. E20260852167 & Indian Patent Application No. 202641078837 (2026).