qnulabs.com

Q→NU
Proactively™
Quantum

QNu Labs Quantum Readiness Starter Kit

From Strategy to Implementation for Enterprise and Defence Leaders

info@qnulabs.com

Starter Kit Overview

The kit will be handed over to customer and prospects in 1:1 meeting with them at their premise, during events, hand it over to genuine prospects who are looking for how to start this quantum safe roadmap journey for them and their organizations, or similar.

1. Quantum Threat Assessment Checklist
2. Industry-Specific Risk Matrix
3. 90-Day Action Plan Template
4. Crypto-Agility Implementation Guide
5. Vendor Evaluation Framework
6. Implementation Checklist Summary

Quantum Threat Assessment Checklist

Infrastructure Vulnerability Audit

Current Encryption Assessment

- [ ] Catalogue all encryption methods currently in use at every layer (database, software, VPN, data center, MAN, WAN, etc.,)
- [ ] Identify RSA, ECC, and other quantum-vulnerable algorithms
  - [ ] RSA key lengths and usage locations
  - [ ] ECC implementations across systems
  - [ ] SSL/TLS certificate dependencies
- [ ] Map data classification levels (Public, Internal, Confidential, Restricted)
- [ ] VPN and secure communication channels
- [ ] Document key management systems and processes
- [ ] Assess third-party vendor encryption standards
- [ ] Document signing and verification systems

Critical Asset Inventory

- [ ] Customer/citizen personal data repositories/Patient data repositories
- [ ] Financial transaction systems
- [ ] Intellectual property databases
- [ ] Communication networks (internal/external- email, messaging, VoIP)
- [ ] Cloud storage and backup systems
- [ ] IoT and connected device networks

- [ ] Authentication systems
- [ ] Digital signatures and certificates
- [ ] Backup and disaster recovery systems
- [ ] Third-party integrations and APIs

Compliance & Regulatory Review

- [ ] Current cybersecurity framework alignment (ISO 27001, NIST, etc.)
- [ ] Industry-specific regulations (RBI, SEBI, FDA, TRAI)
- [ ] Data residency and sovereignty requirements
- [ ] Audit and reporting obligations
- [ ] Cross-border data transfer protocols

Risk Scoring Matrix

Score each category: 1 (Low Risk) to 5 (Critical Risk)

Risk Category	Current Score	Quantum Threat Level	Priority Action
Customer Data Protection	_/5	_/5	High/Medium/Low
Financial Systems	_/5	_/5	High/Medium/Low
IP & Trade Secrets	_/5	_/5	High/Medium/Low
Communication Security	_/5	_/5	High/Medium/Low
Third-party Integrations	_/5	_/5	High/Medium/Low

Total Risk Score: __/50

- **40-50:** Immediate action required
- **30-39:** Accelerated planning needed
- **20-29:** Standard preparation timeline
- **Below 20:** Monitor and prepare strategically

Industry-specific Risk Matrices

Banking & Financial Services

System Component	Quantum Vulnerability	Business Impact	Regulatory Risk	Timeline to Secure
Core Banking System	HIGH	CRITICAL	HIGH	6-12 months
Payment Gateways	HIGH	CRITICAL	HIGH	3-6 months
Customer Portals	MEDIUM	HIGH	MEDIUM	6-9 months
Internal Communications	MEDIUM	MEDIUM	LOW	9-12 months
Data Analytics Platform	LOW	MEDIUM	LOW	12-18 months

Regulatory Considerations

- RBI Guidelines: Master Direction on Cyber Security Framework
- SEBI: Cybersecurity and Cyber Resilience Framework
- IRDAI: Guidelines on Information and Cyber Security

Information Technology & Software

System Component	Quantum Vulnerability	Business Impact	Regulatory Risk	Timeline to Secure
Client Data Centers	HIGH	CRITICAL	HIGH	3-6 months
Software Distribution	HIGH	HIGH	HIGH	6-9 months
Development Environments	MEDIUM	MEDIUM	MEDIUM	9-12 months
Customer Support Systems	MEDIUM	HIGH	MEDIUM	6-9 months
Internal IT Infrastructure	LOW	MEDIUM	LOW	12-18 months

Regulatory Considerations

- MeitY: National Cyber Security Strategy
- STQC: Security testing and certification requirements

Pharmaceutical & Healthcare

System Component	Quantum Vulnerability	Business Impact	Regulatory Risk	Timeline to Secure
Patient Records (EHR)	HIGH	CRITICAL	HIGH	6-12 months
Research Data	HIGH	CRITICAL	MEDIUM	3-6 months
Clinical Trial Systems	HIGH	HIGH	HIGH	6-9 months
Supply Chain Management	MEDIUM	HIGH	MEDIUM	9-12 months
Manufacturing Systems	MEDIUM	MEDIUM	LOW	12-18 months

Regulatory Considerations

- CDSCO: Data integrity guidelines
- **Clinical trial data protection requirements

Telecommunications

System Component	Quantum Vulnerability	Business Impact	Regulatory Risk	Timeline to Secure
Network Infrastructure	HIGH	CRITICAL	HIGH	6-12 months
Customer Data Management	HIGH	CRITICAL	MEDIUM	3-6 months
Billing & CRM Systems	MEDIUM	HIGH	LOW	9-12 months
IoT Device Management	MEDIUM	MEDIUM	MEDIUM	12-18 months
Internal Communications	LOW	MEDIUM	LOW	18-24 months

Regulatory Considerations

- DoT: Telecommunication security guidelines
- TRAI: Consumer data protection requirements
- 5G security enhancements mandated by 2025

Industry-specific Risk Matrices

Public Sector Undertakings (PSUs)

System Component	Quantum Vulnerability	Business Impact	National Security Risk	Timeline to Secure
Citizen data protection audit	HIGH	CRITICAL	HIGH	3-6 months
Inter-department communication security	HIGH	CRITICAL	HIGH	3-6 months
Digital governance platform assessment	HIGH	CRITICAL	HIGH	3-6 months
Critical infrastructure protection review	HIGH	CRITICAL	HIGH	3-6 months
National security communication protocols	HIGH	HIGH	HIGH	3-6 months
Cross-agency quantum security standardisation	MEDIUM	MEDIUM	MEDIUM	3-12 months
Public service delivery security enhancement	MEDIUM	MEDIUM	MEDIUM	3-12 months

Regulatory Considerations

- Digital India security frameworks
- Right to Information Act compliance
- National cybersecurity strategy alignment
- National Security Council: Critical infrastructure protection
- CERT-In: Government security guidelines
- National quantum security standards by 2024-2025

Defence & Aerospace

System Component	Quantum Vulnerability	Business Impact	National Security Risk	Timeline to Secure
Classified information encryption audit	HIGH	CRITICAL	HIGH	3-6 months
Communication systems security review	HIGH	CRITICAL	HIGH	3-6 months
Supply chain security assessment	HIGH	CRITICAL	HIGH	3-6 months
Critical weapons systems protection	HIGH	CRITICAL	HIGH	3-6 months
Quantum-safe military communication networks	HIGH	HIGH	HIGH	3-16 months
Allied nation data sharing security protocols	MEDIUM	MEDIUM	MEDIUM	6-12 months
Strategic asset protection enhancement	HIGH	CRITICAL	HIGH	3-12 months

Regulatory Considerations

- National security classification guidelines
- International defence cooperation security standards
- Export control compliance requirements
- CERT-In: Government security guidelines
- National quantum security standards by 2024-2025

90-day Action Plan Template

Days 1-30: Foundation & Assessment

Week 1: Leadership Alignment

- [ ] Form Quantum Security Task Force
- [ ] Form Quantum Security Task Force
- [ ] Complete initial threat assessment using this checklist
- [ ] Conduct stakeholder interviews (IT, Security, Compliance, Business)

Week 2: Current State Analysis

- [ ] Complete comprehensive asset inventory
- [ ] Map data flows and encryption touchpoints
- [ ] Review vendor contracts for quantum-readiness clauses
- [ ] Assess budget allocation and resource availability

Week 3: Risk Prioritisation

- [ ] Complete industry-specific risk matrix
- [ ] Identify top 5 critical systems for immediate protection
- [ ] Develop initial business case for quantum security investment
- [ ] Schedule vendor consultations and demos

Week 4: Strategy Development

- [ ] Create high-level implementation roadmap
- [ ] Define success metrics and KPIs
- [ ] Establish governance structure and reporting cadence
- [ ] Plan internal awareness and training programs

Days 31-60: Planning & Piloting

Week 5-6: Solution Architecture

- [ ] Design hybrid quantum-classical security architecture
- [ ] Select pilot use cases and test environments
- [ ] Develop technical requirements and specifications
- [ ] Create vendor evaluation and selection criteria

Week 7-8: Pilot Implementation

- [ ] Procure quantum security solutions for pilot
- [ ] Set up test environment and baseline measurements
- [ ] Begin pilot deployment with selected use cases
- [ ] Establish monitoring and performance tracking

Days 61-90: Validation & Scaling

Week 9-10: Pilot Validation

- [ ] Conduct thorough testing of pilot implementations
- [ ] Measure performance impact and security improvements
- [ ] Document lessons learned and best practices
- [ ] Refine implementation approach based on results

Week 11-12: Scale-Up Preparation

- [ ] Develop enterprise-wide rollout plan
- [ ] Secure budget approval for full implementation
- [ ] Create change management and training programs
- [ ] Establish long-term vendor partnerships

ROI Calculator & Budget Planner

Infrastructure Vulnerability Audit

Current Encryption Assessment

Risk Category	Annual Revenue at Risk	Probability	Expected Annual Loss Vulnerability
Customer Data Breach	₹_____ crores	__%	₹_____ crores
IP Theft Financial	₹_____ crores	__%	₹_____ crores
Fraud Regulatory	₹_____ crores	__%	₹_____ crores
Penalties Business Disruption	₹_____ crores	__%	₹_____ crores
Total Expected Annual Loss			**₹_____ crores**

Investment Planning Framework

Implementation Phase	Estimated Cost	Timeline	ROI Expected
Customer Data Breach	₹_____ lakhs	3-6 months	____ %
IP Theft Financial	₹_____lakhs	6-12 months	____ %
Fraud Regulatory	₹_____ crores	12-24 months	____ %
Total Expected Annual Loss	**₹_____ crores**	**24 months**	**___% ROI**

Budget Categories

- **Technology & Licensing:** 40-50% of total budget
- **Professional Services:** 20-30% of total budget
- **Training & Change Management:** 10-15% of total budget
- **Ongoing Support & Maintenance:** 15-20% of total budget

Crypto-agility Implementation Guide

Phase 1: Foundation Building

Algorithm Inventory

- Document all cryptographic implementations
- Identify hard-coded vs. configurable algorithms
- Map dependencies and integration points

Architecture Assessment

- Evaluate current key management infrastructure
- Assess API and interface flexibility
- Review certificate management processes

Phase 2: Hybrid Implementation

Quantum-Safe Algorithm Selection

- NIST Post-Quantum Cryptography standards
- Algorithm performance benchmarking
- Interoperability testing

Gradual Migration Strategy

- Parallel operation of classical and quantum-safe systems
- Performance monitoring and optimization
- Rollback procedures and contingency planning

Phase 3: Full Transition

Enterprise-Wide Deployment

- Coordinated rollout across all systems
- User training and support programs
- Continuous monitoring and updating

Vendor Evaluation Framework

Technical Capabilities Assessment

Criteria	Weight	OEM A Score	OEM B Score	OEM C Score
Quantum Key Distribution	25%	___/10	___/10	___/10
Post-Quantum Cryptography	20%	___/10	___/10	___/10
Integration Capabilities	15%	___/10	___/10	___/10
Performance & Scalability	15%	___/10	___/10	___/10
Security Certifications	10%	___/10	___/10	___/10
Local Support & Services	10%	___/10	___/10	___/10
Total Cost of Ownership	5%	___/10	___/10	___/10

Key Vendor Questions Checklist

- [ ] What quantum-safe algorithms do you support?
- [ ] How do you handle key lifecycle management?
- [ ] What is your upgrade and migration strategy?
- [ ] Do you provide 24/7 support in India?
- [ ] What certifications and compliance standards do you meet?
- [ ] Can you provide customer references in our industry?
- [ ] What is your roadmap for emerging quantum technologies?

Implementation Checklist Summary

Immediate Actions (This Week)

- [ ] Complete threat assessment checklist
- [ ] Calculate potential risk exposure
- [ ] Identify the top 3 critical systems for protection
- [ ] Schedule leadership alignment meeting

Short-term Actions (Next 30 Days)

- [ ] Form quantum security task force
- [ ] Conduct comprehensive asset inventory
- [ ] Develop initial business case
- [ ] Begin vendor evaluation process

Long-term Actions (Next 90 Days)

- [ ] Implement pilot quantum security solution
- [ ] Create enterprise-wide rollout plan
- [ ] Secure budget and resource approval
- [ ] Establish vendor partnerships

Schedule your free 1-hour quantum readiness consultation

QNu Labs Support Services

- **Free Consultation:** Initial quantum risk assessment
- **On-site Workshops:** Customised for your industry and organisation
- **Pilot Implementation:** Guided proof-of-concept deployment
- **24/7 Support:** Ongoing technical and strategic assistance

Q→NU
Proactively™ Quantum

Tomorrow's Quantum Security, Today

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629

India USA Australia Global

info@qnulabs.com