Quantum Readiness

Planning Guide

NOKIA | Quantum FOUNDRY | QUANTUM CORRIDOR®

Quantum-Safe Networking and Communications Checklist

1. Assessment and Discovery

- [ ] **Inventory cryptographic assets**
- [ ] Identify all systems using cryptographic algorithms (e.g., RSA, ECC, DSA)
- [ ] Document all data encryption implementations
- [ ] Map certificate authorities and PKI infrastructure
- [ ] List all VPN implementations and protocols
- [ ] Catalog secure communication channels (TLS/SSL)
- [ ] **Risk assessment**
- [ ] Classify data by sensitivity and retention requirements
- [ ] Identify which systems process high-value data ("harvest now, decrypt later" targets)
- [ ] Estimate timeline to migration based on data protection requirements
- [ ] Document compliance requirements that may be affected by quantum computing

2. Strategy Development

- [ ] **Create quantum-safe transition roadmap**
- [ ] Establish timelines aligned with NIST standardization process
- [ ] Prioritize systems based on risk assessment
- [ ] Allocate budget for transition
- [ ] Identify key stakeholders and responsibilities
- [ ] **Policy updates**
- [ ] Revise cryptographic policy to include quantum-safe requirements
- [ ] Update procurement guidelines for new systems
- [ ] Establish vendor assessment procedures for quantum readiness
- [ ] Develop crypto-agility requirements for future deployments

3. Technical Preparation

- [ ] **Skills development**
- [ ] Train security team on quantum computing threats
- [ ] Educate developers on post-quantum cryptography implementation
- [ ] Prepare IT operations for transition challenges
- [ ] **Testing environment**
- [ ] Set up sandbox for PQC algorithm testing
- [ ] Implement testing protocols for cryptographic transitions
- [ ] Establish benchmarking process for performance comparison

4. Implementation Planning

- [ ] **Algorithm selection**
- [ ] Monitor NIST post-quantum cryptography standardization
- [ ] Select appropriate quantum-resistant algorithms for different use cases
- [ ] Consider hybrid approaches (classical + post-quantum) for transition period
- [ ] **Hardware considerations**
- [ ] Assess performance impact of PQC on existing hardware
- [ ] Identify hardware security modules (HSMs) that support or have roadmaps for PQC
- [ ] Plan hardware upgrades where necessary
- [ ] **Software assessment**
- [ ] Evaluate crypto libraries for PQC support
- [ ] Check vendor roadmaps for quantum-safe updates
- [ ] Identify software dependencies that may require custom solutions

5. Network Infrastructure Updates

- [ ] **Communication protocols**
- [ ] Plan updates to TLS implementations
- [ ] Evaluate quantum-safe VPN solutions
- [ ] Assess impact on network performance (bandwidth, latency)
- [ ] Test protocol compatibility across vendors
- [ ] **Key distribution**
- [ ] Plan transition to quantum-resistant key exchange
- [ ] Evaluate quantum key distribution options (if applicable)
- [ ] Update certificate management systems
- [ ] **Network equipment**
- [ ] Inventory network devices requiring firmware/software updates
- [ ] Check vendor roadmaps for quantum-safe capabilities
- [ ] Develop replacement strategy for unsupported equipment

6. Implementation Execution

- [ ] **Phased rollout plan**
- [ ] Begin with non-critical systems
- [ ] Implement hybrid cryptographic solutions where possible
- [ ] Establish rollback procedures for each phase
- [ ] Schedule maintenance windows for critical infrastructure
- [ ] **Certificate transition**
- [ ] Plan certificate authority updates

- [ ] Schedule certificate replacements
- [ ] Test certificate validation processes
- [ ] **Monitoring and validation**
- [ ] Update security monitoring for new algorithms
- [ ] Implement cryptographic algorithm validation processes
- [ ] Test intrusion detection systems with new protocols

7. Ongoing Management

- [ ] **Cryptographic agility**
- [ ] Implement frameworks allowing easy algorithm replacement
- [ ] Document procedures for rapid cryptographic updates
- [ ] Test cryptographic agility procedures regularly
- [ ] **Vendor management**
- [ ] Include quantum readiness in vendor assessments
- [ ] Require quantum-safe roadmaps from critical vendors
- [ ] Monitor vendor compliance with agreed PQC timelines
- [ ] **Regulatory compliance**
- [ ] Monitor changes in regulatory requirements regarding quantum security
- [ ] Update compliance documentation to reflect quantum-safe implementations
- [ ] Prepare for potential new certification requirements

8. Documentation and Knowledge Management

- [ ] **Updated architecture diagrams** Document new
- [ ] cryptographic implementation details Update network
- [ ] security documentation
- [ ] Revise disaster recovery procedures
- [ ] **Training materials**
- [ ] Create resources explaining quantum computing risks
- [ ] Develop guides for implementing quantum-safe
- [ ] solutions Establish knowledge sharing mechanisms

9. Partner and Customer Communication

- [ ] **External communication plan**
- [ ] Develop messaging regarding quantum-safe transition
- [ ] Create timeline for notifying partners of protocol changes
- [ ] Establish support processes for transition-related issues
- [ ] **Customer education**

- [ ] Provide resources explaining quantum computing threats
- [ ] Share timelines for service updates
- [ ] Offer guidance for customer-side preparations

10. Long-term Strategy

- [ ] **Continuous evaluation**
- [ ] Schedule regular reviews of quantum computing advancements
- [ ] Reassess risk profiles annually
- [ ] Update roadmap based on standardization progress
- [ ] **Research and development**
- [ ] Monitor emerging quantum-resistant technologies
- [ ] Participate in standards development (if applicable)
- [ ] Explore quantum technologies that may provide advantages (QKD, etc.)

Resources:

- NIST Post-Quantum Cryptography Standardization: https://csrc.nist.gov/projects/post-quantum-cryptography
- NSA Cybersecurity Perspectives on Quantum Computing
- ENISA Quantum-Safe Recommendations
- Industry working groups (Quantum-Safe Industry Specification Group, etc.)

Glossary:

- **PQC**: Post-Quantum Cryptography
- **QKD**: Quantum Key Distribution
- **RSA/ECC/DSA**: Current public key cryptosystems vulnerable to quantum computing
- **Crypto-agility**: Ability to quickly switch cryptographic algorithms without major system changes