Fact Sheet

Cogito Group

Quantum Readiness Roadmap

Quantum Readiness Roadmap

Quantum computing is advancing rapidly and has the potential to disrupt industries by solving complex problems that classical computers cannot address efficiently. Being "quantum-ready" refers to preparing organisations, processes, and technologies to handle the impact of quantum computing—especially in fields like cryptography, data security, and advanced computation. Establishing a quantum readiness roadmap ensures organisations are prepared for this upcoming shift.

Roadmap

The following roadmap should be regularly revisited and adjusted as quantum technologies evolve and standards for post-quantum cryptography are finalised.

1. Understand Quantum Computing and Its Impact

- **Quantum Basics:** Quantum computing leverages quantum bits (qubits) that exist in superposition, enabling vastly superior computational power compared to classical systems.
- **Key Quantum Concepts:** Superposition, entanglement, quantum gates, and quantum algorithms such as Shor's and Grover's algorithms.
- **Industry Impact:** Quantum computing may revolutionise fields like cryptography (breaking traditional encryption), logistics (optimising routes), pharmaceuticals (drug discovery), and artificial intelligence (speeding up machine learning).

2. Assess the Risks and Opportunities

- **Cryptography Risk:** Quantum computers can break widely used cryptographic algorithms (RSA, ECC), which necessitates a shift to quantum-resistant algorithms.

- **Data Lifespan Threat:** Any sensitive data encrypted today could be at risk in the future if intercepted and stored until quantum computers become capable of decrypting it.
- **Business Opportunity:** Quantum algorithms offer significant performance improvements for optimisation problems, machine learning, and materials science.

3. Build Awareness Across the Organisation

- **Executive Education:** Ensure leadership understands the strategic importance of quantum technologies.
- **Cross-Functional Teams:** Engage stakeholders from IT, cybersecurity, R&D, and legal to collaborate on assessing and planning for quantum readiness.
- **Industry Monitoring:** Stay informed of developments in quantum computing, particularly breakthroughs in algorithms, hardware, and industry applications.

4. Prioritise Cryptographic Agility

- **Quantum-Safe Cryptography (QSC):** Start implementing cryptographic agility to switch easily between encryption schemes as needed.
- **Post-Quantum Cryptography (PQC):** Research and begin evaluating NIST-approved post-quantum cryptographic algorithms.
- **Inventory & Audit:** Conduct an inventory of existing cryptographic implementations within the organisation and prioritise critical systems for upgrading to PQC.

5. Develop a Long-Term Strategy

- **Research Quantum Algorithms:** Identify algorithms relevant to your industry (e.g. quantum search algorithms for data analysis or quantum optimisation for logistics).
- **Collaborate with Experts:** Engage with academic institutions and quantum computing companies to stay updated and possibly partner on pilot projects.

- **Evaluate Quantum Services:** Assess cloud-based quantum computing platforms (e.g. IBM Q, Google's Quantum AI, Microsoft Azure Quantum) to explore testing quantum algorithms in sandbox environments.

6. Create a Post-Quantum Transition Plan

- **Near-Term (1-3 years):** Focus on education, cryptographic agility, and preparing data protection policies.
- **Mid-Term (3-5 years):** Begin deploying quantum-safe algorithms in high-priority systems, monitor advances in quantum hardware, and evaluate quantum-enhanced solutions for optimisation, AI, and cybersecurity.
- **Long-Term (5+ years):** Adopt full quantum-resistant infrastructure, leverage quantum computing for competitive advantages, and transition to quantum hardware where feasible.

7. Establish Partnerships and Collaborations

- **Engage with Standardisation Bodies:** Work with industry groups (e.g., NIST, ETSI) to align with emerging quantum-safe standards.
- **Collaborate with Tech Providers:** Partner with quantum technology vendors and service providers to gain insights and early access to emerging quantum tools.
- **Consortium Participation:** Join consortia focused on advancing quantum technologies to stay ahead of the curve.

8. Invest in Workforce Training and Skill Development

- **Quantum Computing Skills:** Develop internal quantum expertise by offering training in quantum algorithms, software, and hardware.
- **Cross-Training:** Encourage teams in cryptography, cybersecurity, and IT infrastructure to learn quantum-related skills.
- **Recruitment:** Start attracting talent with quantum computing experience from research institutions and quantum startups.

9. Test and Pilot Quantum Solutions

- **Simulation and Testing:** Utilise quantum simulators or quantum-as-a-service platforms to test quantum algorithms in a controlled environment.
- **Pilot Projects:** Start small with specific use cases where quantum computing can show early benefits (e.g. optimisation in supply chain management or cryptography simulations).

10. Governance, Compliance, and Risk Management

- **Compliance:** Ensure your roadmap aligns with evolving industry regulations on quantum security (e.g. GDPR, HIPAA).
- **Risk Assessment:** Continuously reassess the risk quantum computing poses to your business and adjust strategies accordingly.
- **Incident Response Planning:** Include quantum computing in your cybersecurity incident response planning to address potential quantum-related threats.

Conclusion

A quantum readiness roadmap ensures your organisation is well-prepared for the advent of quantum computing. By prioritising cryptographic agility, investing in talent development, and establishing partnerships, you can position your organisation to mitigate quantum risks while exploring opportunities for innovation.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.