IBM Quantum Safe
→ Telecommunications

IBM Quantum Safe for telecommunications

Safeguard your telco networks and services with quantum-safe cryptographic technology

Telco security in the quantum era

Telecommunications networks and services play an increasingly important role in global communications, digital transformation across industries, emergency response, and national security. With a growing number of cybersecurity attacks on communication service providers (CSPs) recorded globally, maintaining the security and integrity of telco systems in light of evolving risks remains an ongoing critical activity.

Emerging quantum technologies present both an exciting opportunity and a potential risk for the telco industry. Cryptography is used across all telco systems to protect data, infrastructure, and communications. As quantum computers mature, they could tackle some of the world's most complex problems, including the prime factorization of large numbers, which will compromise many of the established encryption algorithms that are currently used in security protocols.

Understanding current and future risks

The security standards and specifications in the telco network space rely on many standards bodies and working groups, including organizations such as 3GPP, ETSI, IETF, and GSMA, to define security algorithms, protocols, and architectures. These cryptographic algorithms and protocols have evolved over decades, with each new generation of technology bringing improvements to security capabilities and performance.

Typically, operators will have numerous technology and business domains, underpinned by multiple technology generations (for example, in many countries mobile networks include 2G, 3G, 4G and 5G capabilities), and potentially hundreds of offerings and thousands of vendors, across networks and the IT landscape. Data in telco systems includes sensitive and valuable information on subscribers, payment details, devices, network equipment, as well as regulatory information related to emergency response and law enforcement. Often the data is distributed across systems in different environments, and across public and private clouds, providing a broad attack surface for cyber threat actors.

This complexity, coupled with a requirement to maintain service continuity, security, and regulatory compliance, means that CSPs and the wider telco supply chain will require careful planning and cross-ecosystem coordination to support the journey toward quantum cyber resilience. According to the Post-Quantum Telco Network Impact Assessment[1], this journey involves addressing four primary business risks to telcos:

"Harvest now, decrypt later" attacks – stealing sensitive data now with the goal of decrypting it with a future cryptographically relevant quantum computer.

Fraudulent authentication – falsifying code signing certificates and digital signatures to tamper with software updates.

Digital signature forgery – manipulating legal history by forging digital signatures.

Key management attacks – targeting key management to compromise data that is stored for a long time.

Benefits of forward planning

There is no definitive date for when quantum computers will challenge existing cryptography. However, quantum technology is evolving at a rapid pace. Governments and regulatory bodies around the world are already establishing guidelines for the transition to quantum-safe cryptography. For example, the National Institute of Standards and Technology (NIST) announced the selection of four quantum-resistant encryption algorithms for standardization, three of which were developed by IBM researchers, with a view to finalizing the standards in 2024.

Forward planning allows telcos to stay ahead of potential privacy breaches, operational disruption, and material reputational damage. In the context of a complex industry operating environment, there are several advantages for telco clients to begin their quantum-safe journey now:

Optimize investment

- Opportunity to leverage technology refresh cycle activities and investments (e.g., 4G, 5G, 6G), improved budgeting and purchasing decisions
- Ability to drive and manage procurement requirements across the telco vendor landscape to future-proof investments
- Phasing to amortize costs over a longer period of time
- Coordination of synergies with parallel, ongoing activities (e.g., PKI evolution)

Mitigate risk

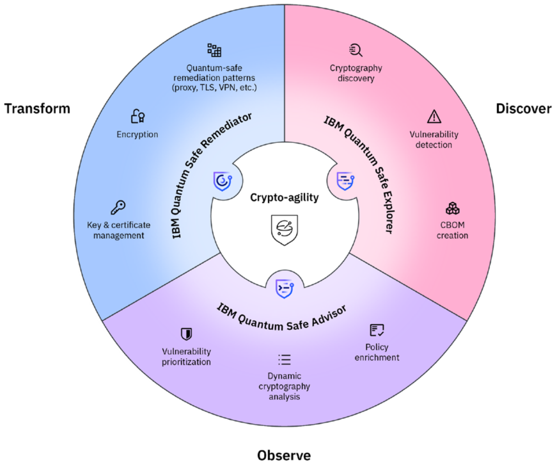
- Stability management (optimize planning around data freezes and change windows)
- Increased opportunities for phasing of testing and implementation cycles
- Preparedness for regulation compliance, as in telco regulation, data privacy, critical infrastructure, and public sector services

Target incremental revenues

- Opportunity for incremental, revenue-generating services; offering quantum-safe services
- Competitive advantage

Building a robust quantum risk posture with IBM Quantum Safe

IBM Quantum Safe is a set of technologies, services, and infrastructure that equips organizations to plan and execute an efficient transition to quantum-safe cryptography.


Transform
Discover
Observe
Crypto-agility
IBM Quantum Safe Remediator
IBM Quantum Safe Explorer
IBM Quantum Safe Advisor
Quantum-safe remediation patterns (proxy, TLS, VPN, etc.)
Encryption
Key & certificate management
Cryptography discovery
Vulnerability detection
CBOM creation
Vulnerability prioritization
Dynamic cryptography analysis
Policy enrichment

Powered by three core technology capabilities, IBM Quantum Safe leverages IBM's industry-leading expertise in quantum, cryptography, security, and telecommunications to enable telco clients to discover, observe, and transform their cryptography and build crypto-agility. Operators identify opportunities for cryptographic modernization and create a plan for adopting quantum-safe security across multiple domains (e.g., device, SIM, network, systems, and infrastructure). IBM Quantum Safe empowers telco clients to begin their quantum-safe transition by taking the following steps, as recommended by the GSMA's Guidelines for Quantum Risk Management for Telco[2]:

Inventory applications and systems to understand where cryptography is used.

Perform a cryptography risk assessment to prioritize vulnerable data and systems.

Identify quantum experts who can stay informed about quantum risks.

Create a quantum-safe transformation strategy.

Learn more about IBM Quantum Safe and start your journey to post-quantum resilience today: https://ibm.biz/BdM8DD

1. Guidelines for Quantum Risk Management for Telco, GSM Association, 2023.
2. Ibid.