

IBM Quantum Safe Technology: Building a Quantum-Resilient Future

Empowering businesses to protect critical data and modernize cryptography for the quantum era. Quantum computing is poised to transform industries—but it also stresses current security infrastructures. Classical cryptographic methods may become vulnerable once quantum computers reach critical power. Organizations handling sensitive data must prepare now for this shift.

Why Prepare Now?

•Data at risk today, exposed tomorrow

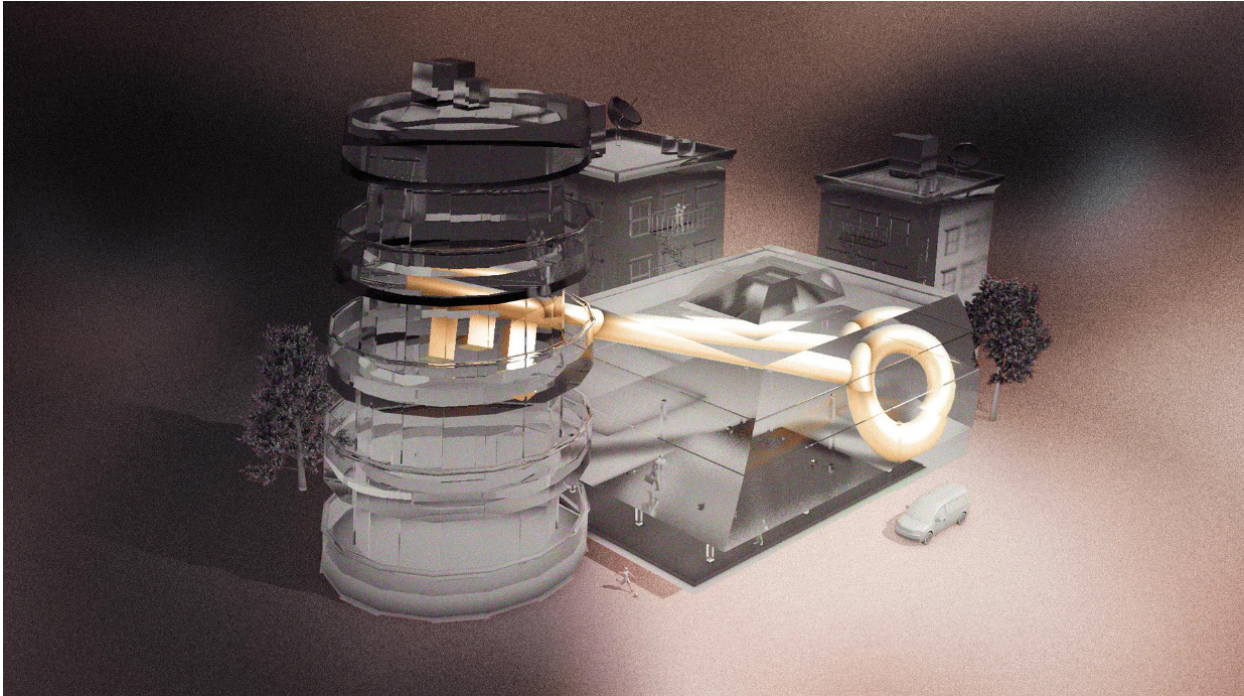
Though large-scale quantum computers are not yet fully realized, cyber actors can use the “harvest now, decrypt later” strategy. Data stolen today might be decrypted in the future.

•The rising cost of data breaches

IBM's Cost of a Data Breach Report 2023 states the global average cost hit USD 4.45 million. The damage from a quantum-enabled cryptographic break could be far more severe.

•Evolving regulation and scarce expertise

Governments globally are issuing mandates toward quantum-safe cryptography. However, many organizations lack visibility into cryptographic usage or a strategic roadmap for transition.



IBM Quantum Safe Technology: Building a Quantum-Resilient Future

IBM Quantum Safe: A Comprehensive Approach

IBM Quantum Safe offers tools, methods, and best practices to help enterprises assess, prioritize, and migrate their cryptographic posture. The framework is built around three phases:

1. Discover

Scan and detect cryptographic usage across your systems. IBM Quantum Safe Explorer examines both source and compiled code, identifies dependencies and vulnerabilities, and builds a Cryptography Bill of Materials (CBOM).

2. Observe

Analyze, monitor, and assess your crypto landscape. IBM Quantum Safe Advisor inspects certificates, cipher suites, algorithm usage, and compliance posture—highlighting risk areas and guiding remediation priorities.

3. Transform

Move toward quantum-safe standards with confidence. IBM Quantum Safe Remediator provides architectural patterns and implementation strategies to replace vulnerable algorithms with quantum-resistant alternatives. It fosters crypto-agility—the agility to adapt to new cryptographic demands with minimal disruption.

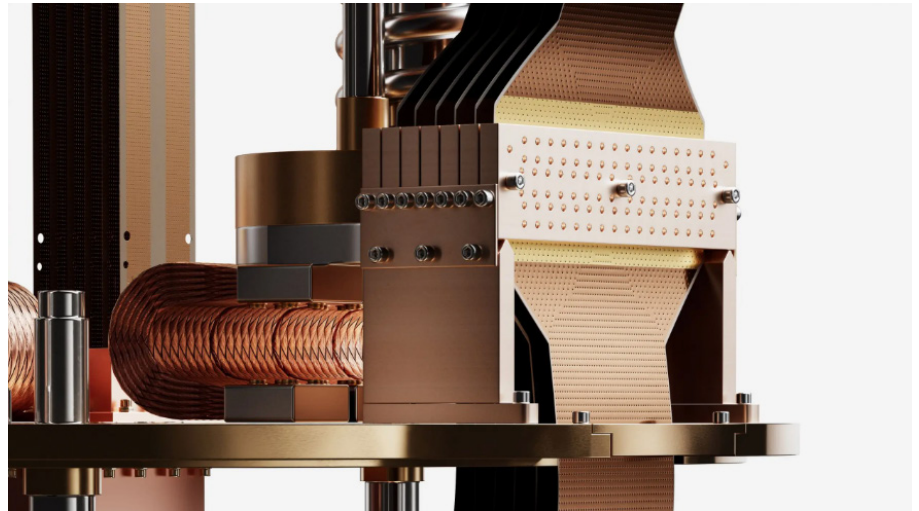
Responsible Quantum: Ethics, Governance & Impact

Quantum computing's power brings great responsibility. IBM's Responsible Quantum initiative emphasizes that quantum technologies must be developed and deployed with foresight, integrity, and societal benefit.

Key principles include:

- Positive societal impact — Prioritize use cases that benefit people and communities.
- Foresight in innovation — Anticipate unintended consequences and avoid harm.
- Transparency and accuracy — Communicate capabilities, limitations, and timelines honestly.
- Consistent principled decision-making — Apply ethics consistently across projects.
- Diversity and inclusion — Build a global quantum ecosystem that reflects diverse backgrounds and perspectives.

IBM already implements contractual terms restricting irresponsible uses of its quantum technologies and aligns its offerings with quantum-safe protections. By integrating responsible quantum principles with quantum-safe cryptography, organizations can pursue the quantum future more ethically and securely.



IBM Quantum Safe Technology: Building a Quantum-Resilient Future

A Trusted Partnership for the Quantum Era

IBM stands at the forefront of quantum innovation—driving progress not only in quantum-safe cryptography, but also in the development of responsible, ethical, and secure quantum technologies.

Through continuous research, collaboration, and industry partnerships, IBM is enabling organizations worldwide to prepare for the quantum era—helping them build resilient, future-proof infrastructures and embrace the next generation of digital security.

Sources

1. IBM Security. Cost of a Data Breach Report 2023.
2. IBM Quantum Safe Technology Overview — <https://www.ibm.com/quantumsafe>
3. IBM Quantum Blog. Defining responsible quantum computing — <https://www.ibm.com/quantum/blog/responsible-quantum>
4. <https://www.ibm.com/quantum/blog/responsible-quantum>