Quantum Technologies @ EY

Strategic Insight | Scalable Solutions
Risk Awareness

October 2025

The better the question. The better the answer. The better the world works.

EY
Shape the future
with confidence

Contents

1

Quantum Technologies @ EY

Quantum Technologies @ EY

Strategic insight | Scalable solutions | Risk awareness

> By collaborating with EY, you will leverage our proven expertise, alliances with industry leaders, and proficiency in implementing the latest quantum technologies and tools to accelerate your quantum journey responsibly.

Partnerships with industry leaders

Long-term relationships with strong external players like IBM Quantum and others

End-to-end offering with modular services

Ability to tailor services in terms of workstream and personalization, from use case development to strategy and roadmaps

A team of quantum experts

A global network of over 700 professionals with a strong interest on quantum innovation

Success stories

We have carried out several projects with international clients and collaborated with partners in industry and academia

Responsible development

Quantum governance strategy and data strategy to facilitate privacy, transparency and explainability

Our use cases

EY Global Inn. + NCSR Demokritos + IBM Quantum
Quantum DNA Sequencing
Life Sciences

EY Global Inn. + NCSR Demokritos + IBM Quantum
Crop Identification
Sustainability

EY Global Inn. + NCSR Demokritos + IBM Quantum
Quantum Games

EY Global Inn. + QCi
Portfolio Optimization MVS
Financial Services

EY Global Innovation
Portfolio Optimization
Financial Services

EY Global Innovation
Quantum Safety
Financial Services

EY Global Innovation
Quantum Readiness & Innovation Framework
Private & Public Sector

How can we help you?

Computation Simulation	QUANTUM RESEARCH AND DEVELOPMENT PROGRAM	QUANTUM STRATEGY DEVELOPMENT
Communications	QUANTUM CYBERSECURITY RISK ASSESSMENT	QUANTUM RESISTANT NETWORK
Sensing/Metrology	INTEGRATION WITH DATA & ANALYTICS USE CASES	
Enablement	QUANTUM LAB SETUP AND DEVELOPMENT	AWARENESS & TRAINING ACTIVITIES

Quantum Safe:
EY's Post-Quantum Cryptography Lab

2

Quantum security

Security timeline in the quantum age

- Quantum decryption might be only five years away.
- All systems need to be quantum secure TODAY – "Harvest now, decrypt later".

Governments, regulators and security experts are proactively addressing the impending threat by:

  - Raising awareness,
  - Developing quantum secure algorithms and standards
  - Preparing regulations

for a secure transition to Post-Quantum Cryptography (PQC).

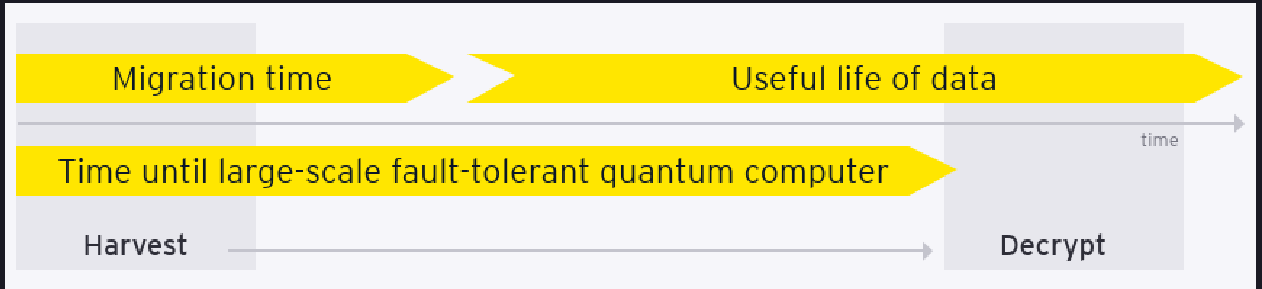
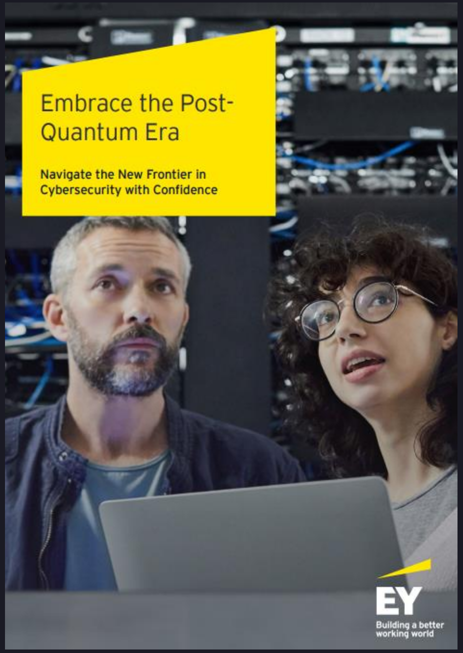


Figure 6. Mosca's theorem – "Harvest Now, Decrypt Later" attack

Why we need to act NOW!

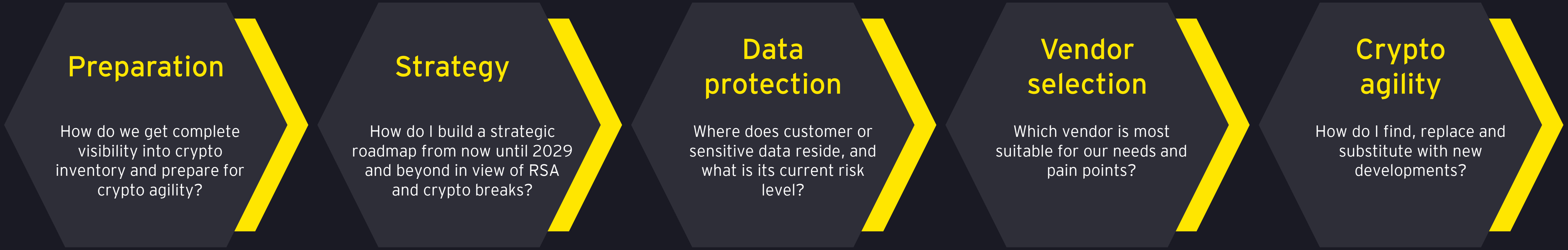
- The lifecycle of critical data, assets and infrastructure often exceeds the anticipated timeline for quantum decryption.
- Transitioning to an agile post-quantum cryptography (PQC) environment requires time and presents complex challenges.
- The lack of PQC compliance will pose significant reputational and operational risks in the near future.
- Early adoption guarantees business continuity and is significantly more cost-effective.

- The National Institute of Standards and Technology (NIST) emerged as a guiding beacon, leading the standardization of PQC.
- NIST has announced they will deprecate current cryptography algorithms by 2030. Approved post-quantum cryptographic (PQC) algorithms will become the new standard.*


Embrace the Post-Quantum Era
Navigate the New Frontier in Cybersecurity with Confidence
EY
Building a better working world

*Source: NIST IR 8547 Transition to Post-Quantum Cryptography Standards

Client concerns point to adoption friction and compliance challenges



Preparation

How do we get complete visibility into crypto inventory and prepare for crypto agility?

Strategy

How do I build a strategic roadmap from now until 2029 and beyond in view of RSA and crypto breaks?

Data protection

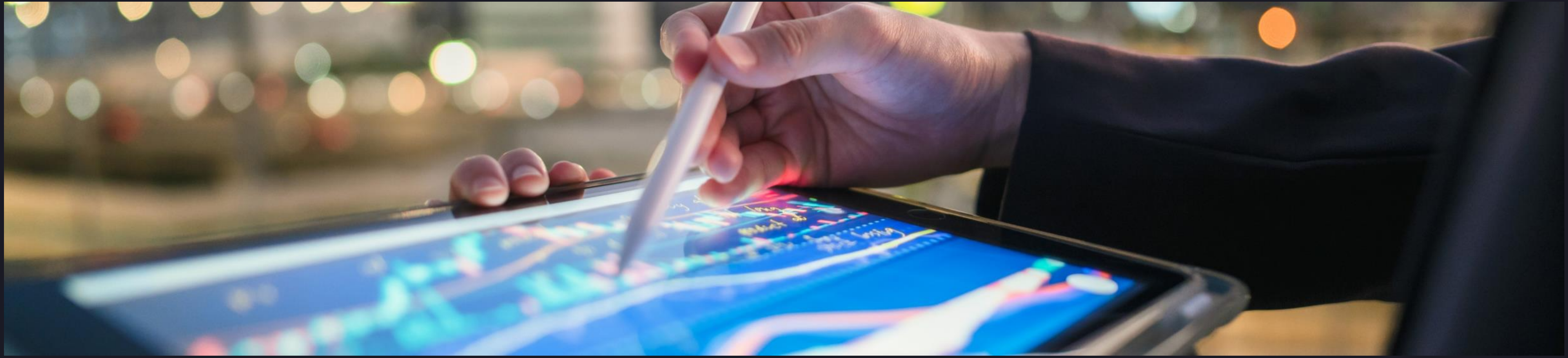
Where does customer or sensitive data reside, and what is its current risk level?

Vendor selection

Which vendor is most suitable for our needs and pain points?

Crypto agility

How do I find, replace and substitute with new developments?



EY Quantum Safe

MVP suite of accelerators

> Organizations are prioritizing protection against oncoming quantum threats and the existing threats of harvested data for future encryption.

Inventory

- Aggregate and trace quantum at-risk digital supply chain assets.
- Integration with PQC offering scanners and inventory tooling.
- Detect and identify at-risk systems and underlying data sources.

Risk assessment

- Prioritize assets for migration based on criticality of data exchange.
- Migration planner and dashboard for critical data and assets.
- Define custom rules and profiles tailored for client's risk profiles.

Modernization

- Remediate vulnerable assets and the associated infra pipeline.
- Integration with PQC offerings to swap in quantum safe vendor solutions.
- Quantum cyber defense & cryptanalysis capabilities.

3

Quantum Computing Use Cases for Finance

Quantum computing use cases

Indicative use cases in finance

Monte Carlo simulations

Quantum computing can speed up Monte Carlo simulations, a critical method for assessing financial risks and uncertainty. This acceleration can enable financial institutions to evaluate and manage risk exposures more efficiently.

Credit scoring

Quantum methods can improve credit scoring models by considering a wider range of data sources and complex patterns, resulting in more accurate assessments of creditworthiness and reducing loan default risks for financial institutions.

Credit risk analysis

By utilizing quantum computing, financial institutions can assess and manage credit risks and forecast defaults with greater precision. This enables more effective risk mitigation strategies and improves overall portfolio management.

Fraud detection

Quantum computing can enhance fraud detection capabilities by analyzing vast amounts of transactional data and detecting patterns that might indicate fraudulent activities, enabling proactive risk mitigation and prevention.

Anti-money laundering

Quantum algorithms can be used to analyze financial transactions and identify patterns associated with money laundering and illegal activities. This enhances regulatory compliance and strengthens the security of financial systems.

Portfolio optimization

Quantum algorithms can assist in optimizing investment portfolios by efficiently analyzing a broad range of assets, risk factors and constraints. This can help institutions achieve better risk-adjusted returns and improve allocation strategies.

Asset pricing

Quantum computers can be used to accurately price financial assets by considering complex models and market parameters. This can assist in valuing derivatives, options and other securities more effectively.

Index tracking

Quantum computing can be used to optimize the tracking of indices, allowing investment firms to create and manage index-based investment products more effectively.

Quantum Portfolio Optimization

Management of investment portfolios with QC

Description

Portfolio optimization is the process of selecting the best distribution of financial assets while maximizing the expected return and minimizing the financial risk.

Motivation

This is an NP-hard combinatorial optimization problem and extremely difficult to solve classically, but not with a quantum approach.

The shift from traditional classical solutions to quantum mean-variance-skewness (QMVS)

Limitations and challenges of classical approach

- ***Model limitations for real-world portfolios***: Traditional mean-variance models ignore skewness and struggle with integer constraints.
- Machine learning models often lack strong constraint fidelity and create new audit and governance difficulties.
- Traditional mean-variance ignores upside asymmetry, and when non-convex features are added, it often relies on relaxations/penalties resulting in unstable weights.

QMVS advantage for the ideal solution

- Incorporating mean, variance and skewness in optimization improves upside asymmetry and captures richer risk profiles.
- Quantum computing addresses cubic and skew-aware problems natively, enabling enhanced portfolio positioning and better risk-adjusted returns.
- An ideal approach uses exact skew terms, supports hard constraints, requires fewer parameters and promotes reproducibility and explainability.

Highlights

- **EY & QCi** Skew-Aware Portfolio Optimization
  - Results were obtained using QCi's Dirac-3 Quantum Machine
- Key Highlights of our comparison:
  - Quantum-MVS balances high Sharpe with minimal drawdown and concentrated bets.
  - Markowitz excels in raw return but suffers deeper drawdowns and lower skew capture.
  - Skew-aware methods consistently outpace benchmark risk-adjusted performance.

NASDAQ-100 analysis (2023–2025) shows skew-aware portfolios delivering:

Method	Sharpe Ratio	Max Drawdown	Assets Selected	Runtime
MVS-QCi	2.61	8.2%	4 (concentrated)	0.001s
MV	2.23	12.1%	101 (diversified)	0.015s
Full-MVS	2.45	9.8%	~80 (skew-aware)	0.045s
Lin-MVS	1.89	15.3%	~60 (moderate)	0.003s
Benchmark	1.20	22.5%	101 (equal-weight)	N/A

4

Quantum Strategy & Risk

EY's Quantum Readiness and Innovation Framework

Quantum Readiness and Innovation Framework (QRIF)

Quantum Awareness | Readiness | Innovation

> Organizations exploring quantum technologies often struggle to develop and implement their quantum strategy and roadmap, and to measure its impact.

What is QRIF?

- A model that evaluates the impact of quantum technologies on organizations, addressing the limitations of traditional methods by integrating multiple dimensions, such as Economic Diversification & Resilience, Quantum Confidence, Value Generation and Maturity, into a unified assessment framework.
- It assesses critical facets of their quantum journey collectively, providing a macro-level index that tracks the entire quantum adoption journey.
- It provides a detailed and strategic final score, reflecting the technological impact of quantum while considering an organization's preparedness and risk profile.
- It provides a comprehensive evaluation of quantum awareness and readiness for:
  - Ecosystems and markets
  - Commercial and industrial organizations
  - Government and public sector

What does QRIF offer?

- A holistic view of quantum awareness, readiness, and organizational adoption
- Insights for developing and executing a quantum strategy and implementation roadmap
- Key focus areas for future growth and their anticipated impact on organizational performance indicators
- Early adoption of quantum technologies to seize opportunities and proactively manage risks

5

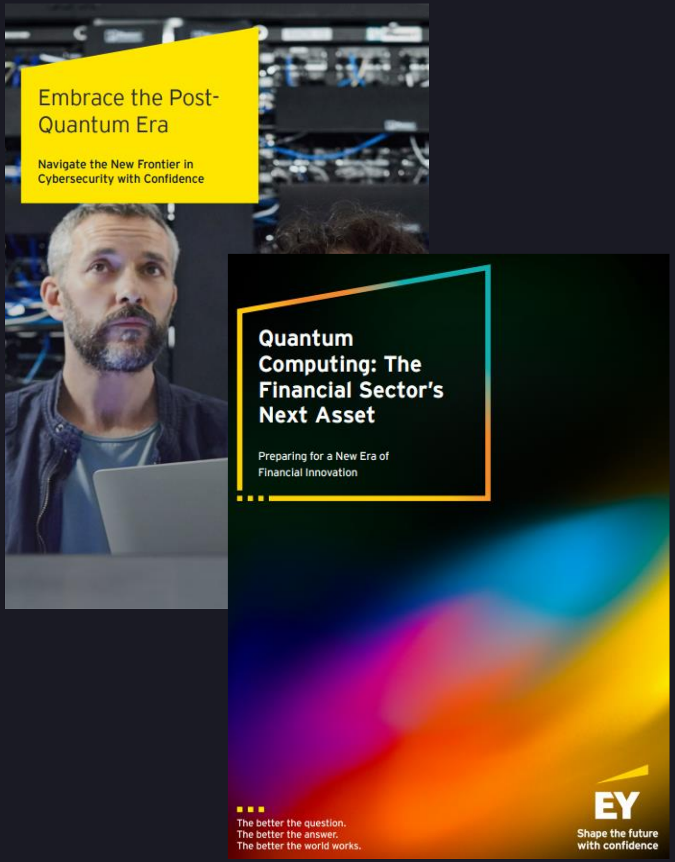
Summary

Now is the time to get ready for quantum technology

Disruptive innovation | Incredible opportunities | Significant risks

Why you should get quantum-ready now

- Quantum technology is advancing at an unprecedented speed.
- Quantum tech leaps forward in 2025, quantum advantage is just around the corner.
- The quantum ecosystem is expanding annually, fueled by substantial public and private investments.
- Quantum adoption requires time, early adopters are rewarded.
- Quantum cybersecurity risks (e.g., "harvest now | decrypt later" attacks) raise concerns for institutions and industries, necessitating immediate risk mitigation.
- Quantum Innovation: Quantum technologies are set to drive innovation and disruption across industries and the entire value chain.



Embrace the Post-Quantum Era

Navigate the New Frontier in Cybersecurity with Confidence

Quantum Computing: The Financial Sector's Next Asset

Preparing for a New Era of Financial Innovation

The better the question.
The better the answer.
The better the world works.

EY
Shape the future with confidence

6

EY Global Innovation's Quantum Lab

The EY Global Innovation Quantum Lab

Accelerate quantum adoption across EY and for our clients

Joe Depa
EY Global Chief Innovation Officer
United States

Rodrigo Madanes
Next Frontier Tech/AI Leader
United States

Rodrigo.Madanes@ey.com

Kartheek Solipuram
Quantum Innovation Lead
United States

Kartheek.Solipuram@ey.com

Evangelos Karamatskos
Quantum R&D Leader
Greece

Vaggelis.Karamatskos@gr.ey.com

The EY Global Innovation Quantum Lab published a whitepaper on the opportunities and the impact of quantum computing in the financial sector.

Key topics include:

- Use cases and application areas of quantum computing in FS
- A roadmap for quantum adoption in financial institutions

Quantum Computing: The Financial Sector's Next Asset

Preparing for a New Era of Financial Innovation

The better the question.
The better the answer.
The better the world works.

EY
Shape the future with confidence

2024/25 NIST Post-Quantum Encryption Standards

NIST unveils Quantum-Resistant Encryption Standards to secure the future of digital information

- NIST standards provide the necessary tools to protect the digital infrastructure in the quantum era.
- NIST encourages transitioning to these new standards immediately, as the integration process can take years.
- Enable organizations to protect electronic information from quantum threats, facilitating data security and privacy
- Adoption of standards to future-proof encryption systems, safeguarding data privacy & integrity

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)*

- Based on CRYSTALS-KYBER and primary standard for encryption (**FIPS 203**)
- Protects against large-scale fault-tolerant quantum computer attack
- Provides secure key establishment thus allowing for **encryption and authentication**

ML-DSA (Module-Lattice-Based Digital Signature Algorithm)**

- Based on CRYSTALS-Dilithium and primary standard for secure digital signatures (FIPS 204)
- Strong Authenticity: Unique & non-repudiable signatures
- Provides data integrity by detecting unauthorized modifications

SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)***

- Based on SPHINCS+ and as a backup method for FIPS 204 (FIPS 205)
- Provides integrity check through hash-based stateless signatures.
- Stronger & simpler data integrity checks without needing sensitive information

FN-DSA (Fast Fourier over NTRU lattices based Digital Signature Algorithm)

- Planned for late 2024 based on FALCON algorithm
- Aimed to be a hybrid DSA with stronger security against classical and quantum attacks

HQC (Hamming Quasi-Cyclic Code-Based Key Encapsulation Mechanism)

- Finalized standardization expected in 2027
- HQC will serve as a backup for ML-KEM, the main algorithm for general encryption

*Source: *FIPS203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard*

**Source: *FIPS 204 - Module-Lattice-Based Digital Signature Standard*

***Source: *FIPS205 - Stateless Hash-Based Digital Signature Standard*

Deprecation of traditional cryptography standards

NIST IR 8547

- NIST has announced they will deprecate current cryptography algorithms by 2030. Approved post-quantum cryptographic (PQC) algorithms will become the new standard.*

Algorithm Family	Security Strength	Example Algorithms	Transition
Asymmetric Cryptography (classical)	112 bits	RSA (≤2048) ECDH (≤256bits) ECDSA(≤256bits)	Deprecated after 2030 Disallowed after 2035
	≥128 bits	RSA (>2048) ECDH (>256bits) ECDSA(>256bits)	Disallowed after 2035
Symmetric Cryptography (classical)	112 bits	SHA-224	Disallowed after 2030
	≥128 bits	SHA-256 AES-128	Allowed
Asymmetric Cryptography (Post-Quantum)	NIST Post-Quantum Cryptography Categories	ML-KEM ML-DSA SLH-DSA	Allowed

***Source:** *NIST IR 8547 Transition to Post-Quantum Cryptography Standards*

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2025 Ernst & Young LLP.
All Rights Reserved.

2510-10359-CS
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com