Quantum Preparedness Assessment (QPA) Report

User Email: developer@qse.group

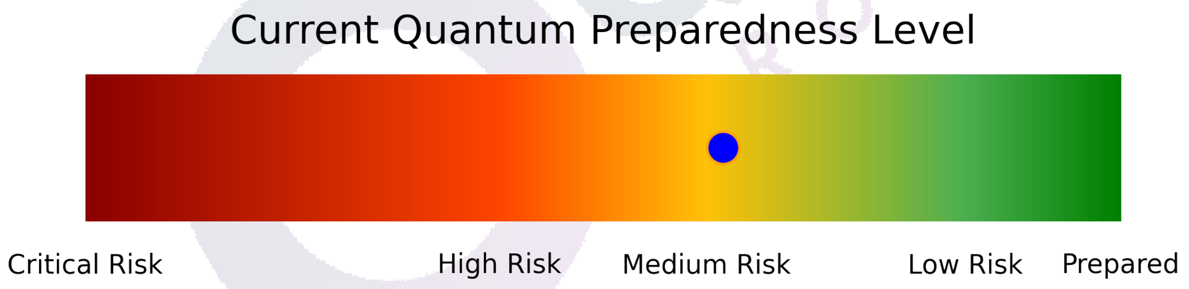
Selected Tier: BRONZE

Score: 41.25/67.00

Quantum Readiness: 61.57%

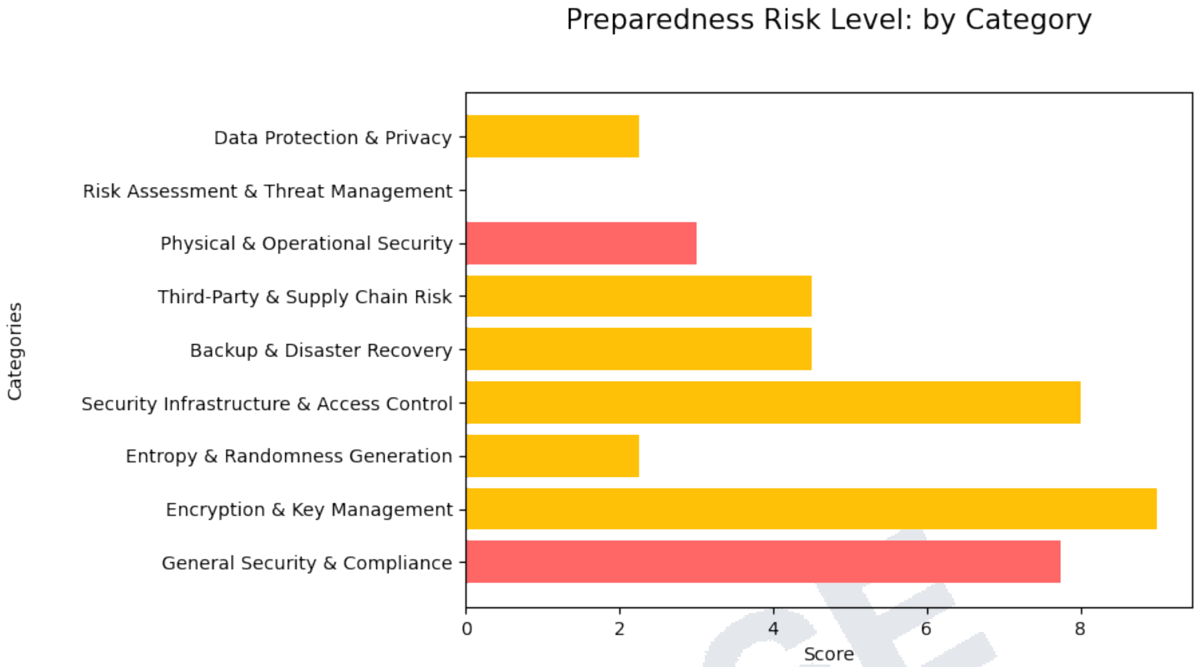
Risk Level: ⚠ Medium Risk (Needs Improvements)

Visit QSE Group



Explanation: Current Quantum Preparedness Level

The chart illustrates the current quantum preparedness level, showcasing a spectrum from critical risk to being fully prepared. The gradient highlights various risk categories, moving from red for critical and high risk to green for low risk and prepared. The blue dot indicates the current preparedness level, positioned in the medium risk area. This suggests that while precautions may be in place, there are still significant vulnerabilities that require attention. Organizations or stakeholders can interpret this as a call to action, seeking improvements in strategies and measures to transition toward a safer, more prepared status. The emphasis on medium risk underscores the importance of ongoing efforts in enhancing quantum preparedness, as neglecting this could lead to potential challenges in the future. Overall, the visual representation effectively communicates the need for proactive measures to mitigate risks associated with quantum technology.

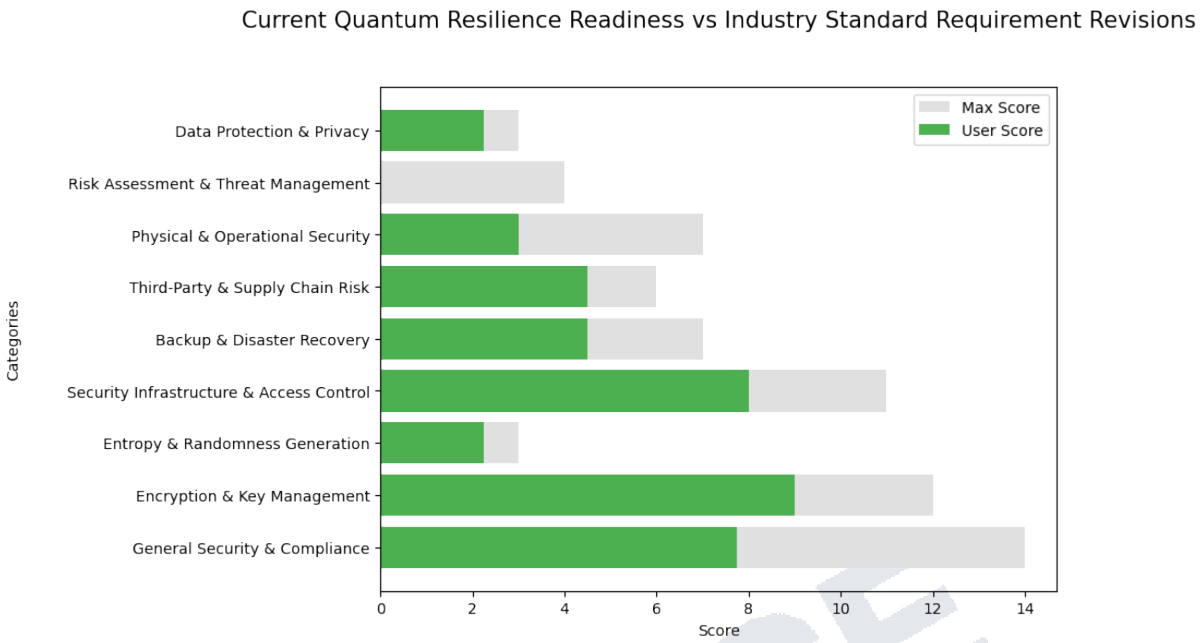


Explanation: Preparedness Risk Level: by Category

The chart illustrates various categories of preparedness risk levels, highlighting areas where attention is needed. Notably, "Data Protection & Privacy" scores the highest, suggesting organizations are well-equipped in this area. Conversely, "General Security & Compliance," along with other categories like "Encryption & Key Management" and "Physical & Operational Security," shows significant vulnerability, indicated by lower scores.

Categories such as "Risk Assessment & Threat Management" and "Third-Party & Supply Chain Risk" reflect a balanced score, suggesting a moderate need for improvement. Additionally, "Backup & Disaster Recovery" often falls in the middle range, emphasizing its importance but indicating that enhancements could further bolster preparedness.

Overall, the data highlights a clear divide: while certain areas show strong readiness, critical aspects of security and compliance require urgent attention to mitigate risks effectively. Focus on strengthening the lower-scoring categories is essential for a more comprehensive risk management strategy.

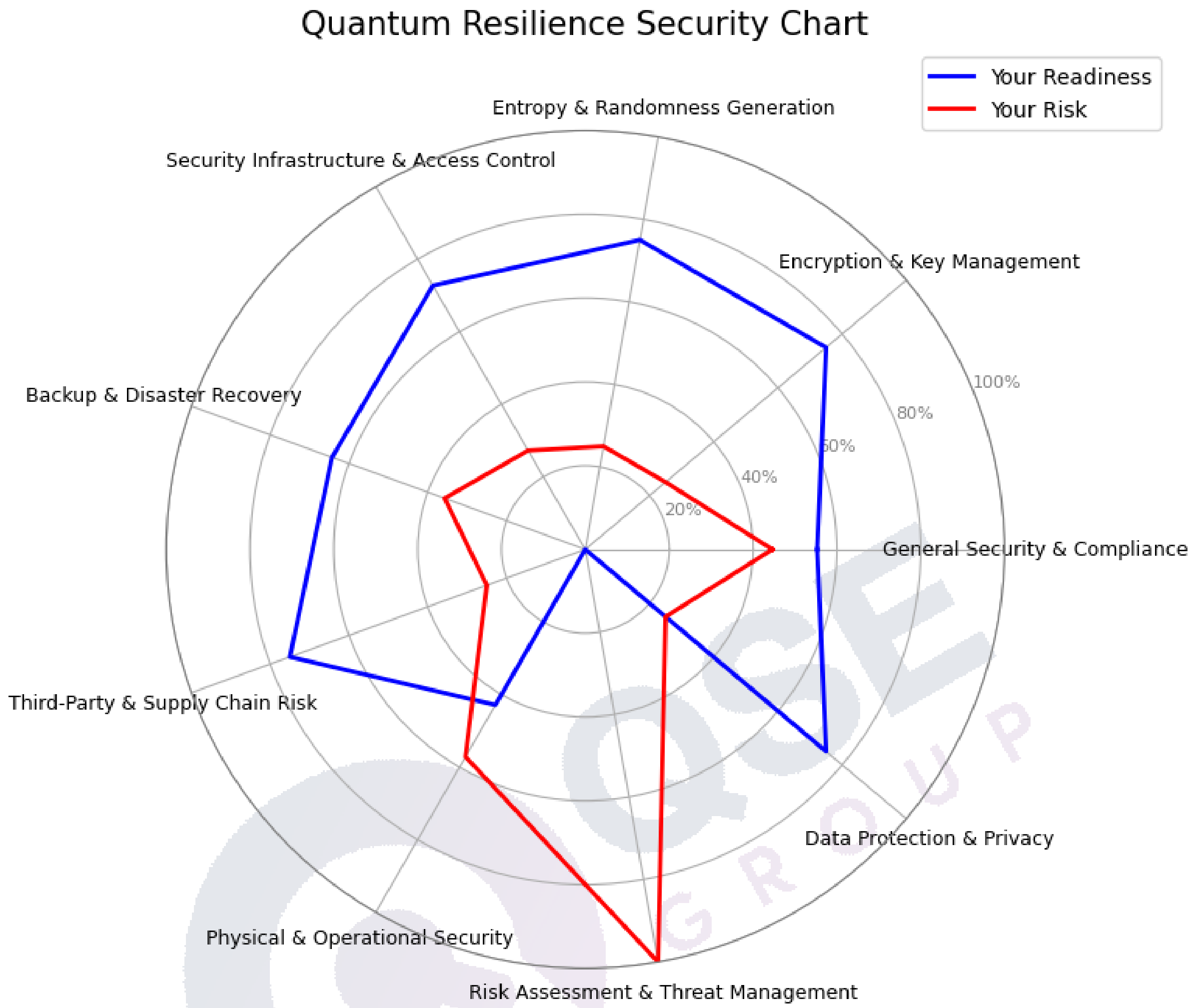


Explanation: Current Quantum Resilience Readiness vs Industry Standard Requirement Revisions

The chart compares current quantum resilience readiness against required industry standards across various security categories. It highlights that most categories show a noticeable gap between the scores achieved by users and the maximum potential scores. Data Protection & Privacy stands out as a strong area, with users demonstrating readiness that is relatively close to the ideal standard.

In contrast, categories like Encryption & Key Management and Security Infrastructure & Access Control reveal significant need for improvement, as user scores fall short of the maximum potential. Additionally, Backup & Disaster Recovery and Third-Party & Supply Chain Risk showcase a mixed performance but still indicate areas that require more focus to reach compliance with industry standards.

Overall, while some areas are faring well, there is a clear need for enhanced efforts in critical security domains to align with evolving industry expectations. This suggests a proactive approach is necessary for organizations aiming to improve their quantum resilience.

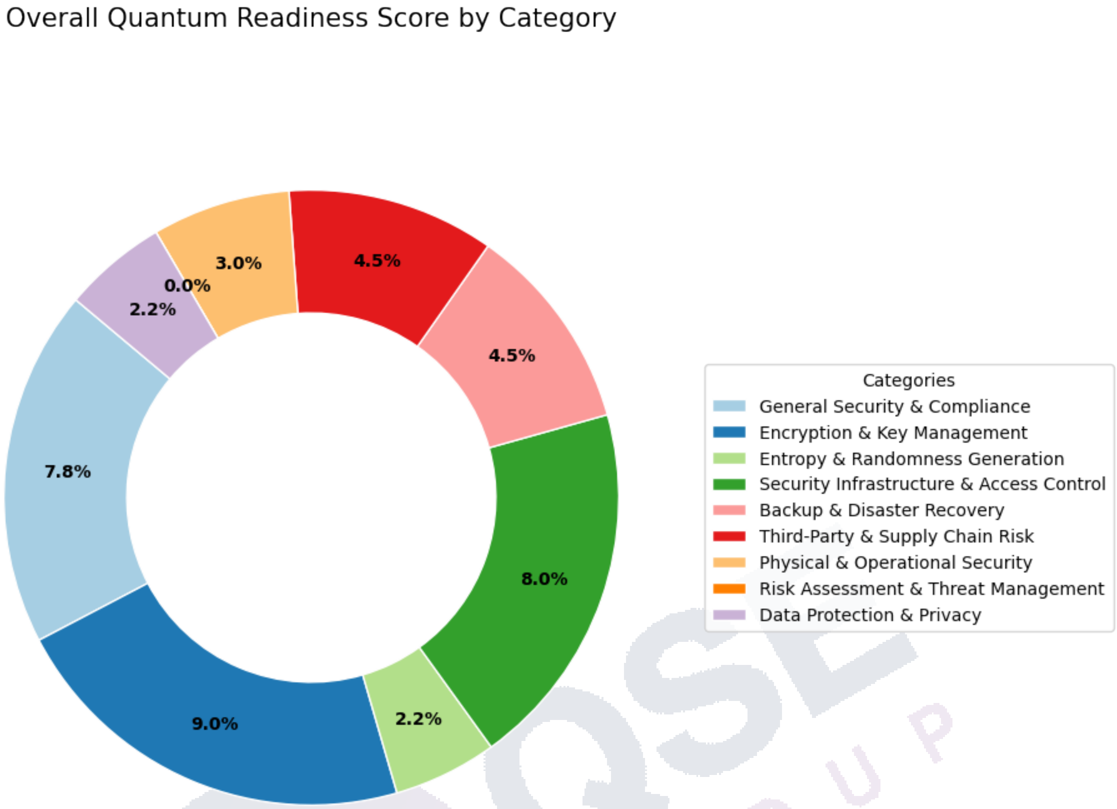


Explanation: Quantum Resilience Security Chart

The chart presents a comparison between an organization’s readiness and its associated risks in the context of quantum resilience security. It has two main lines: one representing your readiness (in blue) and the other indicating your risk (in red).

A key insight is that while the organization shows reasonably strong readiness in areas like backup and disaster recovery and encryption management, there are significant risks in several domains, such as general security and compliance, and risk assessment. The stark contrast between the blue and red lines in these areas highlights vulnerability, suggesting a need for stronger controls and strategies to mitigate risks.

Additionally, areas like data protection and supply chain risk show a more balanced relationship, but still indicate that improvements can be made to enhance overall security posture. Addressing these gaps could boost readiness levels and mitigate potential threats more effectively. Overall, the chart underscores the importance of aligning readiness with risk management efforts to ensure a robust quantum resilience strategy.



Explanation: Overall Quantum Readiness Score by Category

This chart illustrates various categories' contributions to an overall quantum readiness score. Notably, "General Security & Compliance" and "Backup & Disaster Recovery" emerge as significant areas, each contributing substantially to the total score. "Third-Party & Supply Chain Risk" and "Entropic & Randomness Generation" also hold essential roles but are comparatively lower.

Some categories, such as "Encryption & Key Management" and "Data Protection & Privacy," show minimal contributions, suggesting that these areas may require more focus to enhance overall quantum readiness. A couple of categories, like "Physical & Operational Security," are at the lower end of the score spectrum, highlighting potential vulnerabilities.

In essence, the chart indicates a need for a balanced approach to quantum readiness, emphasizing the importance of bolstering weaker areas while maintaining strengths in more robust categories. This analysis can guide organizations in prioritizing resources and strategies to improve their quantum security posture.

Quantum Risk Assessment Summary

The user's total security score of 41.25 out of possible 67.0 indicates a medium level of risk, suggesting a notable room for improvement in their cybersecurity infrastructure. Despite implementing some measures, such as adhering partially to various industry regulations and employing security controls from CIS and NIST, the security posture is far from robust. The lack of a comprehensive regulatory compliance strategy, along with a disturbingly heavy reliance on external consultants for managing cybersecurity systems, and RMF points towards vulnerability in the General Security & Compliance criteria. This, coupled with the potential threat of substantial financial strain and reputational damage in the event of data breaches could increase the risk quotient drastically.

Their cryptographic strategy seems relatively strong in comparison, with the active use of robust encryption algorithms such as RSA-2048 and AES-256 GCM. However, a potential loophole is the use of RSA-1024 with insecure hashing for data encryption at rest, which urges a need for a more solid encryption protocol. The existing use of TLS 1.2 for data in transit, despite possessing certain weak ciphers, is another red flag that could undermine data security. Parallelly, entropy originates from /dev/urandom with reseeding, which mandates continuous monitoring to ensure the randomness in key generation isn't compromised.

Moving onto infrastructure resilience and access control, while firewalls are in place, the conspicuous lack of active monitoring could amplify the susceptibility to threats. The presence of multiple internet-facing components and cloud dependencies only reinforces this risk. However, it's commendable that multifactor authentication is mandatory for all users, a promising aspect in their security paradigm. With regard to backup & disaster recovery, even though minor breaches with no data loss were reported, the storage of encryption keys with backups is a critical vulnerability that could potentially result in unauthorized data access.

In the domain of third-party and supply chain risk, the presence of several third-party services along with ambiguous security reviews and inconsistent compliance enforcement among vendors contributes towards risk enhancement. Further, identified potential risks including disgruntled employees or external hostile entities hint towards a precarious state of physical & operational security. The absence of responses related to swatting incidents and the quantum impact on the company impede a comprehensive risk evaluation in these respective areas.

Lastly, concerning data protection & privacy, while existing controls offer some protection, the confirmed presence of security gaps coupled with the need for additional measures to safeguard sensitive data underscores a crucial factor in risk accumulation. The organization's security strategy, thus, requires urgent augmentation to navigate these multifaceted, interconnected risks. In summary, though there are a few security strengths in place, a high number of exploitable weaknesses demand immediate attention to fortify their quantum security posture and thereby reduce cyber threats.

Top 20 Actionable Insights

- Transition towards complete compliance with industry regulations or compliance standards
- Establish a formal and consistent usage of either CIS or NIST controls
- Enhance internal expertise in cybersecurity systems and RMF management
- Plan for financial reserves or insurance to cover potential regulatory fines
- Transition from RSA-1024 to RSA-2048 for data-at-rest encryption
- Remove weak ciphers from the TLS 1.2 protocol for data-in-transit encryption
- Appoint a dedicated cybersecurity team for active firewall monitoring
- Apply strict security measures for all internet-facing components and cloud services
- Encrypt backups independently of their storage, ensuring encryption keys are stored separately
- Improve contingency planning for minor to severe data breaches
- Conduct regular security reviews and monitoring of all third-party services
- Standardize and enhance enforcement of security compliance for all vendors
- Develop risk mitigation strategies for potential internal and external threats
- Train employees on the potential risks of swatting and preventive measures
- Define and assess the impact of Quantum-related cyber incidents to establish mitigation strategies
- Implement additional controls to secure personal, health, and financial data
- Ensure stringent security procedures for entropy sources to avoid predictable key generation
- Establish stronger access control policies including routine audits of privileged accounts
- Develop a robust disaster recovery and business continuity plan
- Implement a regular schedule for security risk assessments and threat management.

How QSE Group Can Help

QSE Group is a leader in quantum-secure encryption, specializing in next-generation solutions that safeguard sensitive data from emerging quantum threats. With a dedicated team of cryptographers, security engineers, and compliance experts, we help businesses future-proof their cybersecurity strategies. Our approach is structured around three key pillars:

Assessing Quantum Vulnerabilities:
Through in-depth risk assessments, we identify weak points in your cryptographic infrastructure and operational security.

Implementing Quantum-Resilient Solutions:
We integrate cutting-edge post-quantum cryptographic algorithms that meet or exceed industry security standards.

Ensuring Compliance & Continuous Monitoring:
We align your security framework with evolving global regulations, offering ongoing monitoring and adaptability as new threats emerge.

What Services We Offer

QSE Group provides a comprehensive suite of quantum-secure solutions tailored to enterprises, financial institutions, and high-security organizations. Our offerings include:

Post-Quantum Cryptographic Transition Planning:
We help organizations transition from traditional encryption (RSA, ECC, AES) to quantum resilient encryption.

Fully Proprietary Quantum Proof Cloud Storage:
We provide Immutable Decentralized Cloud Storage, safeguarding your data with storage that cannot be over-encrypted by ransomware. QSE’s decentralized approach ensures continuous access to your data while providing unbreakable encryption that resists quantum computing power.

Quantum Preparedness Assessments:
Our team cevaluate the client's current encryption, entropy, security protocols, and preparedness for both current and future quantum-based security threats, offering recommendations to ensure quantum resilience and data-immutability.

Entropy as a Service (EaaS):
Leveraging advanced QRNG (Quantum Random Number Generation), we ensure cryptographic randomness for robust security. QSE’s Entropy as a Service offers quantum-proof, true randomness for encryption key generation, ensuring your data stays safe today and into the future. Our solution easily integrates with your existing security infrastructure without the need for disruptive overhauls.

Cybersecurity Strategy Consulting & Risk Mitigation:
We work closely with IT and security teams to develop a custom roadmap for quantum security resilience.

Why You Should Take Action Now

The emergence of quantum computing is no longer theoretical—it's an imminent reality. Organizations that delay their transition to quantum-safe security face critical consequences, including permanent data exposure, legal non-compliance, and operational disruptions. The longer an organization waits, the harder and more costly it becomes to secure its infrastructure. Transitioning to post-quantum cryptography (PQC) is not an option—it is a necessity.

Data Exposure Risks:
Quantum computers will eventually break RSA, ECC, and other classical cryptographic methods. Encrypted data harvested today (Harvest Now, Decrypt Later) will be vulnerable once quantum computing reaches a practical threshold. Organizations storing sensitive customer data, financial records, or intellectual property must act now to prevent irreversible breaches.

Regulatory Compliance Pressure:
Governments and compliance bodies like NIST, NSA, and GDPR are enforcing new regulations requiring organizations to transition to post-quantum cryptography. Failing to meet these security mandates could result in **severe legal penalties, non-compliance fines, and reputational damage**. Organizations must implement quantum-resistant cryptographic strategies to maintain compliance.

Operational Disruption:
Companies that do not plan for PQC migration in advance will face significant operational challenges when legacy cryptographic systems become obsolete. Without a clear roadmap, businesses risk extended downtime, loss of encrypted data, and unanticipated security failures. **Being proactive ensures business continuity and smooth integration with future security standards.**

Financial Risks & Increased Costs:
The cost of a quantum-induced data breach could be catastrophic, leading to financial losses in the millions due to regulatory fines, customer lawsuits, and operational recovery expenses. In contrast, implementing quantum-resilient solutions **now** is significantly more cost-effective than reacting after a security failure.

Competitive Disadvantage:
Industry leaders are already transitioning to quantum-safe cryptography. Falling behind in quantum security adoption means falling behind in the market. Clients, partners, and investors prioritize security-first organizations. Proactively securing data ensures a competitive edge and strengthens trust in digital operations.

Irreversible Threats:
Unlike traditional cybersecurity threats that can be patched post-incident, **quantum threats are irreversible.** Once an adversary has obtained encrypted data through quantum attacks, it cannot be recovered or secured retroactively. The only solution is preemptive migration to post-quantum cryptography.

Partnering with QSE Group:

QSE Group specializes in post-quantum cryptography, providing organizations with the tools and expertise needed to make a seamless transition to quantum-resistant security. By taking action today, your organization ensures compliance, prevents future security breaches, and fortifies itself against an uncertain digital future.

User Responses

General Security & Compliance

Question: Which industry regulations or compliance standards does your organization follow?

Selected Answer: No formal compliance, but partial adherence

Question: Which security frameworks does your organization follow?

Selected Answer: Ad-hoc use of CIS or NIST controls

Question: Do you have the expertise onsite to integrate, monitor, maintain, audit your Cybersecurity systems and RMF?

Selected Answer: Cybersecurity team has limited RMF expertise, depend heavily on external consultants for monitoring and compliance

Question: Could a data breach to your organization lead to regulatory fines or lawsuits that strain financial resources?

Selected Answer: A breach could trigger regulatory fines and lawsuits, leading to substantial financial strain and reputational damage

Encryption & Key Management

Question: Which encryption algorithms does your organization use for Data at Rest?

Selected Answer: RSA-1024 with insecure hashing

Question: Which encryption algorithms does your organization use for Data in Transit?

Selected Answer: TLS 1.2 with some weak ciphers

Question: Is your organization using RSA encryption? If yes, what key size is used?

Selected Answer: RSA-2048

Question: Is your organization using AES encryption? If yes, what mode is used?

Selected Answer: AES-256 GCM

Entropy & Randomness Generation

Question: What is the source of entropy for generating encryption keys?

Selected Answer: /dev/urandom with reseeding

Security Infrastructure & Access Control

Question: Does your organization use firewalls to protect network traffic?

Selected Answer: Firewall exists but no active monitoring

Question: How exposed is the system to external networks (e.g., internet-facing applications, cloud services)?

Selected Answer: Multiple internet-facing components and cloud dependencies exist, with unmitigated security measures in place

Question: Are multi-factor authentication (MFA) and strong password policies enforced?

Selected Answer: MFA is mandatory for all users in our organization

Backup & Disaster Recovery

Question: Has your organization experienced data breaches in the past 12 months?

Selected Answer: Minor breaches with no data loss

Question: Are backups encrypted before storage?

Selected Answer: Encryption keys stored with backups

Third-Party & Supply Chain Risk

Question: How many third-party integrations or dependencies exist in your current system?

Selected Answer: Several third-party services, with security reviews in place but require some monitoring

Question: Are your vendors contractually required to meet security compliance standards?

Selected Answer: Most vendors are required to meet security compliance standards, but enforcement and audits are inconsistent

Physical & Operational Security

Question: Are there known threats of violence to your employees or organization (e.g., insider threats, activist groups, disgruntled employees)?

Selected Answer: We have identified some potential risks, such as disgruntled employees or external groups

Question: Have there been cases of swatting (fraudulent emergency calls leading to armed responses) against staff or executives?

Selected Answer:

Risk Assessment & Threat Management

Question: What would be the level of impact Quantum related cyber incidents, such as data breaches, would have in terms of damaging the company’s reputation, leading to loss of business deals?

Selected Answer:

Data Protection & Privacy

Question: How vulnerable is personal, health, or finance data, to exposure through a system breach on your services?

Selected Answer: Sensitive data is protected, but some security gaps exist, and additional controls are needed to reduce breach risks

Who we are?

QSE Group & Scope Technologies Corp

Scope Technologies Corp is an innovation-driven company headquartered in Vancouver, Canada. We specialize in quantum security, AI, and decentralized cloud infrastructure. Our mission is to build secure, scalable, and intelligent systems for a digital-first world.

QSE Group is our flagship platform providing Quantum Security Entropy as a Service (EaaS). It offers advanced quantum-resilient encryption, decentralized IPFS-based storage, and enterprise-grade APIs for developers and organizations looking to secure their data against current and future cyber threats.

Our Key Focus Areas:
- Quantum-Resilient Encryption: Secure cryptography designed to resist quantum attacks.
- Decentralized Cloud Storage: IPFS and Filecoin-based solutions ensuring availability and immutability.
- Entropy-as-a-Service: API access to true quantum randomness for robust encryption key generation.

Learn more

Visit QSE Group
Visit Scope Technologies