Luxoft
A DXC Technology Company

How does a bank become quantum cybersecure?

by **Duncan Alexander**, Product Director, Core Banking, Luxoft

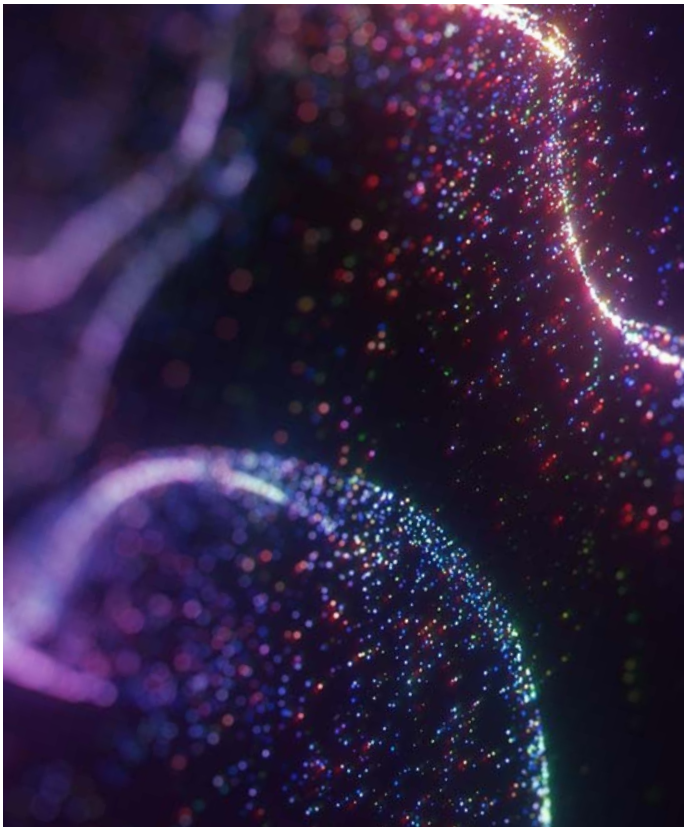
In brief

- The race to devise quantum-resistant cryptography is on. The National Institute of Standards and Technology (NIST) is endeavoring to standardize post-quantum cryptographic algorithms. Fortunately, the banking industry is providing support so its systems can implement quantum-safe encryption ASAP
- Financial institutions are launching pilot programs with quantum-safe algorithms and meshing them with existing cybersecurity practices in preparation for future quantum activities. Many banks have already started trials to gauge the efficiency and security of these algorithms under real-world conditions
- According to BCG, quantum computing could add **$450-$850 billion** in incremental value to the economy over the next 15-30 years

Quantum computing is set to eclipse some of the greatest technological advances in living memory, including cellular networks, Wi-Fi routers and the transistor radio.

It's a quantum leap into multiple future states — known knowns, known unknowns and unknown unknowns — that will allow us to answer complex questions far in excess of our current capabilities.

This rapidly evolving technology is already redefining cybersecurity, risk management and financial operations. And banks must leverage these coming innovations holistically to sharpen profitability and organizational resilience.



But...

The things that make quantum computers (and therefore banking) super powerful, like **quantum superposition and entanglement**, also make current cryptographic defenses (and therefore banks) super vulnerable:

- Public key infrastructures (**PKIs**) protect digital communications and financial transactions. They depend on the compute complexities of factoring large prime numbers, of which, quantum computers are uniquely capable
- **Shor's algorithm** is a quantum algorithm for integer factorization. With a sufficiently powerful quantum computer, a state actor could theoretically use Shor's algorithm to break RSA encryption (a cornerstone of modern cybersecurity) before quantum-safe cryptosystems can be universally deployed. Alternatively, classically encrypted (e.g., public-key cryptography) information could be scraped and stored for decryption at a later date

Developing quantum-resistant cryptography

Unsurprisingly, the race to devise quantum-resistant cryptography is on. The National Institute of Standards and Technology (**NIST**) is endeavoring to standardize post-quantum cryptographic algorithms. Fortunately, the banking industry has thrown its considerable weight behind the initiative to ensure financial systems are in pole position for the implementation of quantum-safe encryption.

Even so, integrating cyber agility with system modernization will be a massive undertaking for top-tier banks. It will involve the entire cast of financial services players and standards bodies and will be supported by cross-industry cooperation at all levels.

Here are three reasons for getting quantum ready now:

- Quantum computers will transform banking value chains, enabling rapid market share gains and greater profitability
- The learning curve is steep, so fast followers could easily overspend playing catch-up
- An in-house center of competency will take years to establish and produce sufficient talent

Use cases in banking

- **Encryption and cryptography:** While it's true that quantum computing could make traditional encryption obsolete, it can also enhance banking cybersecurity. Quantum key distribution (**QKD**) uses quantum mechanics to allow two parties to share a secret key, demonstrably protected against computational strikes

- **Fraud detection:** The ability to analyze massive datasets at quantum speed enables real-time fraud detection, minimizing the time fraudulent transactions remain hidden

- **Risk analysis and management:** Rapidly solving optimization problems promotes more sophisticated risk management, potentially saving billions by averting crises and improving decisioning

- **Portfolio optimization:** Simulating complex financial systems with quantum algorithms helps banks analyze risk and resolve asset pricing with lightning speed and accuracy. This could transform portfolio management by supporting the virtually instant analysis of complex investment narratives to determine an optimal asset mix

Quantum numbers

- The global enterprise quantum computing market was valued at $1,370.82 million in 2020 and is expected to reach **$18,336.45 million** by 2030, registering a CAGR of 29.7% from 2021 to 2030

- According to BCG, quantum computing could add **$450-$850 billion** in incremental value to the economy over the next 15-30 years

- Significant investments in quantum technologies by leading banking players like JPMorgan Chase and Goldman Sachs highlight the potential impact of quantum computing. A recent McKinsey report logged investment in quantum technologies at $2.35 billion in 2022. It also reported that financial services (and other industries) stand to gain up to **$1.3 trillion** in value by 2035

Pilots and partnerships

But banks are not sitting back twiddling their thumbs, waiting for the good times to roll. They're launching pilot programs with quantum-safe algorithms and meshing them with existing cybersecurity practices in preparation for future quantum activities. Many institutions have started trials to gauge the efficiency and security of these algorithms under real-world conditions.

Partnerships between research companies and technology providers are mushrooming, translating quantum research into practical business expertise. Now, tech firms are partnering with banks to establish possible use cases, design quantum algorithms and test developments on authentic quantum computers. And the first applications won't be far behind. For instance, **JPMorgan Chase** has teamed up with IBM to experiment with quantum algorithms in financial use cases.

In due course, quantum literacy and expertise must be embedded throughout the enterprise. In addition, quantum task forces — IT specialists, cybersecurity experts and financial analysts — should be mobilized to evaluate new quantum applications and threats.

Approach and deployment

Quantum computing is imminent, and banking leaders need to view this mega opportunity with a mix of guarded optimism and planned investment. Quantum technologies will likely become the linchpin of banks' financial strategies.

Which quantum computer would suit your business?

Different quantum computers solve different problems and fall into three categories: Quantum annealing, noisy intermediate-scale quantum (NISQ) computing and fault-tolerant universal quantum computing.

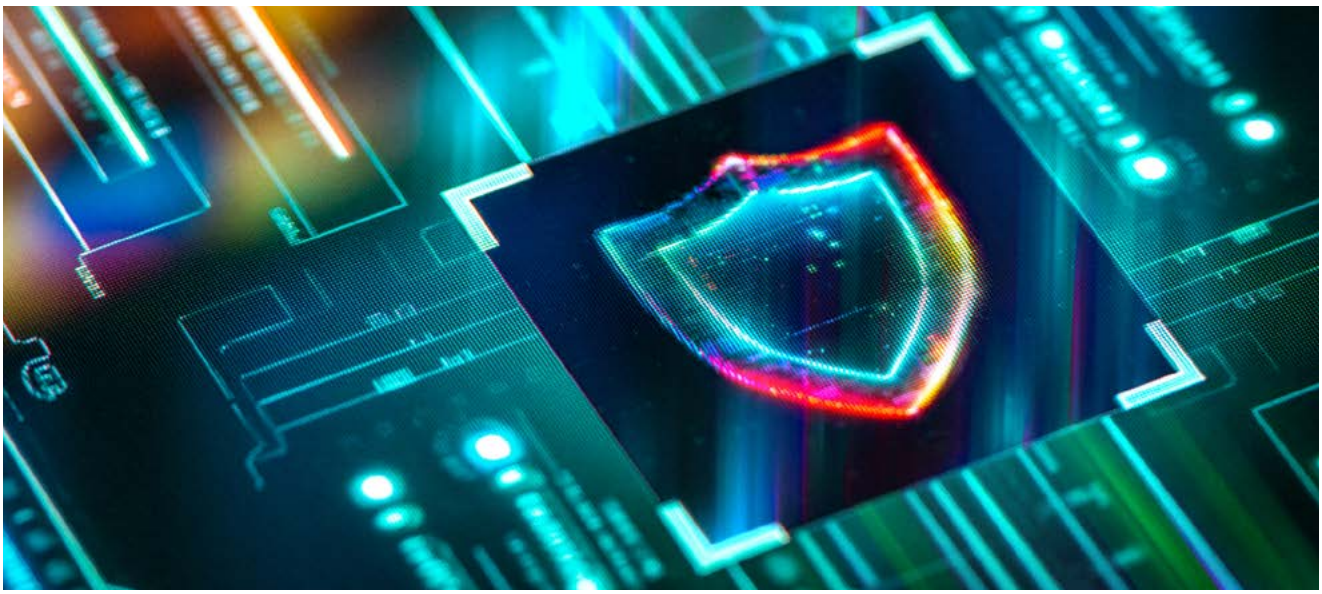
Received wisdom states that quantum annealing is not a true quantum computer, offering only a slight advantage over traditional computers. Also, the development trail for quantum annealing doesn't lead to our ultimate goal — fault-tolerant, universal quantum computers.

Many new algorithms are being adapted for NISQ computers, making them the best bet for delivering a momentary commercial advantage. And, unlike quantum annealing, NISQs aim for fault-tolerant universal quantum computers that handle significant business and technical problems exponentially faster than contemporary devices.

The heart of the matter

Quantum computing's mounting influence on banking is a given, and its root and branch impact on cybersecurity, data analysis and financial modeling will be intense. Those who manage the change judiciously and proactively will gain an invaluable market advantage.

But it's not enough to be on nodding terms with the fundamentals. Banks must prepare thoroughly because the competition for quantum primacy is not solely about speed; it's about having the insight and understanding to transform security, grasp complexity and exploit quantum computing in its entirety to secure your banking future.



IBM z16, Hogan and quantum-safety ready

So, what can we do to protect sensitive information and maintain essential application and infrastructure integrity in the face of future cyberthreats and traditional hostile actors?

As we've seen, although practical quantum computing is down the road a ways, we need to develop quantum-safe cryptographic strategies now. At the same time, we still have to consider the business and social impact. Integrating cyberagility with system modernization will be a massive undertaking for top-tier banks, involving every financial services player and standards body (e.g., **NIST**) and will be supported by through-the-line, cross-industry collaboration.

Any classically encrypted (e.g., public-key cryptography) wire-tappable communications are vulnerable and already at risk, the idea being to "harvest data now, decrypt later" when quantum decryption techniques are finally realized. The IBM z16 provides extra protection by encrypting data wherever it resides — at rest, in-flight and now, in use, with fully homomorphic encryption.

The IBM z16 is quantum-safe ready. IBM has implemented quantum-safe cryptography in the z16 to protect against potential future threats from quantum computers. The system leverages algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium, which have been selected by **NIST** for standardization. These efforts ensure that the IBM z16 can secure data against the advanced computational capabilities of quantum computers, making it a **forward-thinking solution** for cybersecurity.

Mainframe resilience: For decades, mainframes have formed the spine of banking operations. They provide robust processing capabilities, super resilience and unparalleled security. Mainframes handle massive transaction volumes with ease. According to IBM, they process something like **30 billion** transactions a day, plus **87%** of all credit card transactions, highlighting their critical role in banking.

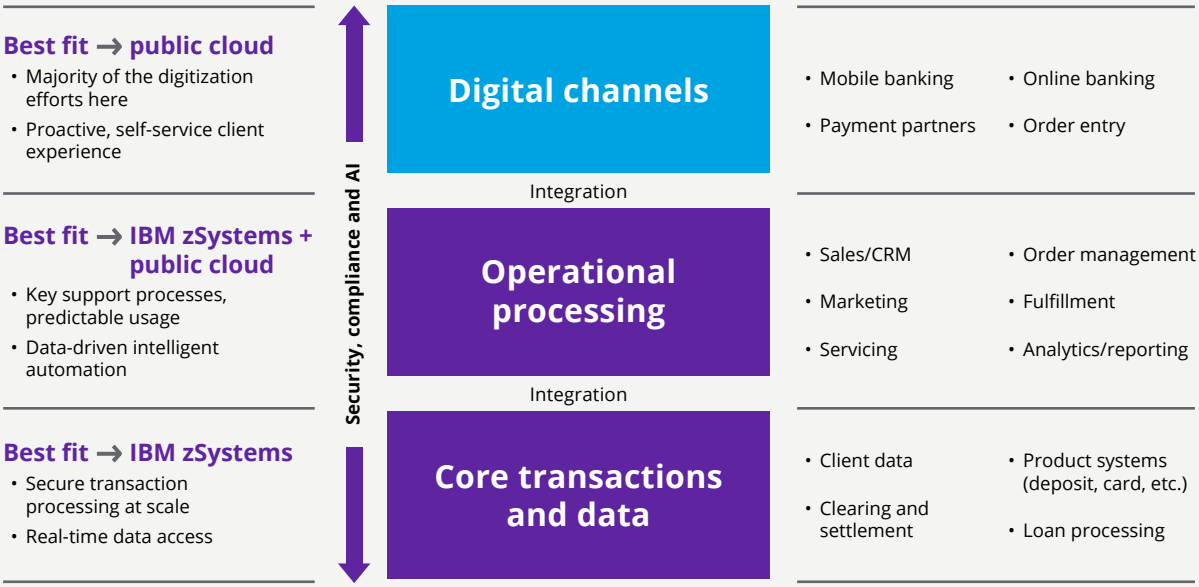
Hybrid flexibility: Hybrid cloud architecture combines public cloud flexibility with private cloud security and on-prem infrastructure. It allows banks to scale resources on demand, rapidly responding to market developments. Gartner predicts that by 2025, more than **90%** of enterprises will have a hybrid cloud infrastructure and platform. However, fewer than 10% have an effective multi-cloud strategy to address complexity, attain simplicity and take advantage of the opportunity.

Mainframe hybrid cloud solution

Integrating mainframes with hybrid cloud architecture offers the best of both worlds: mainframe reliability, security, cloud scalability and innovation potential.

"Cloud migration is gathering serious momentum." So says a 2023 Celent survey of financial institutions. Migration to the public cloud includes moving from legacy on-prem applications to the public cloud, hybrid cloud, public cloud on IaaS, and public cloud on PaaS and SaaS. But balance is everything. It's about placing the right workloads in optimal locations while maintaining operational resilience.

A best-fit approach across IBM Z and cloud: Banking



Some technologies and processes, such as workplace systems that post and retrieve information with minimal data exchange, are better suited to the cloud. On the other hand, heavier, more complex solutions that manage massive amounts of data and transaction volumes are better on-prem and run on a mainframe.

Horizontal applications (especially customer-facing, front-office technology) are also moving to the cloud. These solutions often require real-time data and customer interaction for sales and service and usually have low data requirements. The same is true for mobile/online banking, call-center technology, Salesforce, CRM and advisory relationship solutions that combine agent-assisted sales and service engagement with digital self-service.

Mainframe hybrid cloud implementation helps modernize on-prem infrastructure, enabling greater automation, expanded self-service capabilities and flexible workload deployment and management.

Security and compliance

Security breaches can have catastrophic consequences, so the mainframe's reputation for stiffened security is an attractive feature. Its ability to handle encryption and security protocols at scale is unmatched — an IBM Z mainframe can process up to **12 billion** encrypted transactions a day.

Complying with regulations like GDPR and PCI DSS is a must for banks. The mainframe's robust audit and compliance tools offer a sheltered environment that helps meet the exacting requirements. This is crucial because a single oversight can bring hefty penalties and reputational scrutiny.

Availability and reliability

Downtime is banking's nemesis. Fortunately, mainframe systems are noted for maintaining decades-long business continuity. They offer high-availability features such as IBM Parallel Sysplex, which enables banks to run a cluster of up to 32 servers in parallel, ensuring high performance and continuous availability (even during maintenance or upgrades).

This reliability is essential for "always on" banking. For instance, a central European bank reported an impressive 99.99% availability after integrating mainframe systems, underlining their extraordinary reliability.

Innovation and agility

The agility a hybrid cloud model provides is a primary driver for digital innovation. Mainframe systems offer a stable, high-performance foundation. At the same time, integration with cloud services enables banks to experiment with the latest front-end technologies and generative AI, machine learning (ML) and advanced analytics without disrupting core banking functions. Banks can deploy a combination of ML cloud models to score on mainframe transactions to enhance the customer experience, improve risk management and tackle fraud.

Cost-effective modernization

Modernizing IT infrastructure is expensive. Notably, a cost-effective mainframe hybrid cloud strategy allows banks to modernize without discarding existing investments and expand mainframe capabilities with cloud service agility. In fact, a leading U.S. bank leveraged this architecture to modernize several of its workplace applications, achieving a 70% reduction in processing time and significant cost savings.

Enhanced data management and analytics

The importance of effective data management is well known, and mainframes offer superior capabilities in managing vast data volumes. Banks can use cloud analytics tools to glean actionable data insights while their mainframe systems ensure that high-quality, high-volume data is processed efficiently.

A long-standing Luxoft client, a large multinational bank, integrates mainframe data with cloud analytics to gain real-time insights into customer behavior, improving decision-making and customer service.

Simplifying IT complexity

Inevitably, as a bank grows, its infrastructure becomes increasingly complex.

Cloud costs also increase, e.g., mounting transaction volume and platform management. Consequently, banks are looking to accelerate hybrid cloud efficiency and procure the appropriate internal and external resources to make this happen. A recent report into the escalating cost of cloud computing showed that spending had overtaken security as the #1 management challenge, and a lack of resources/ expertise was next in line.

Scalability and hybrid flexibility

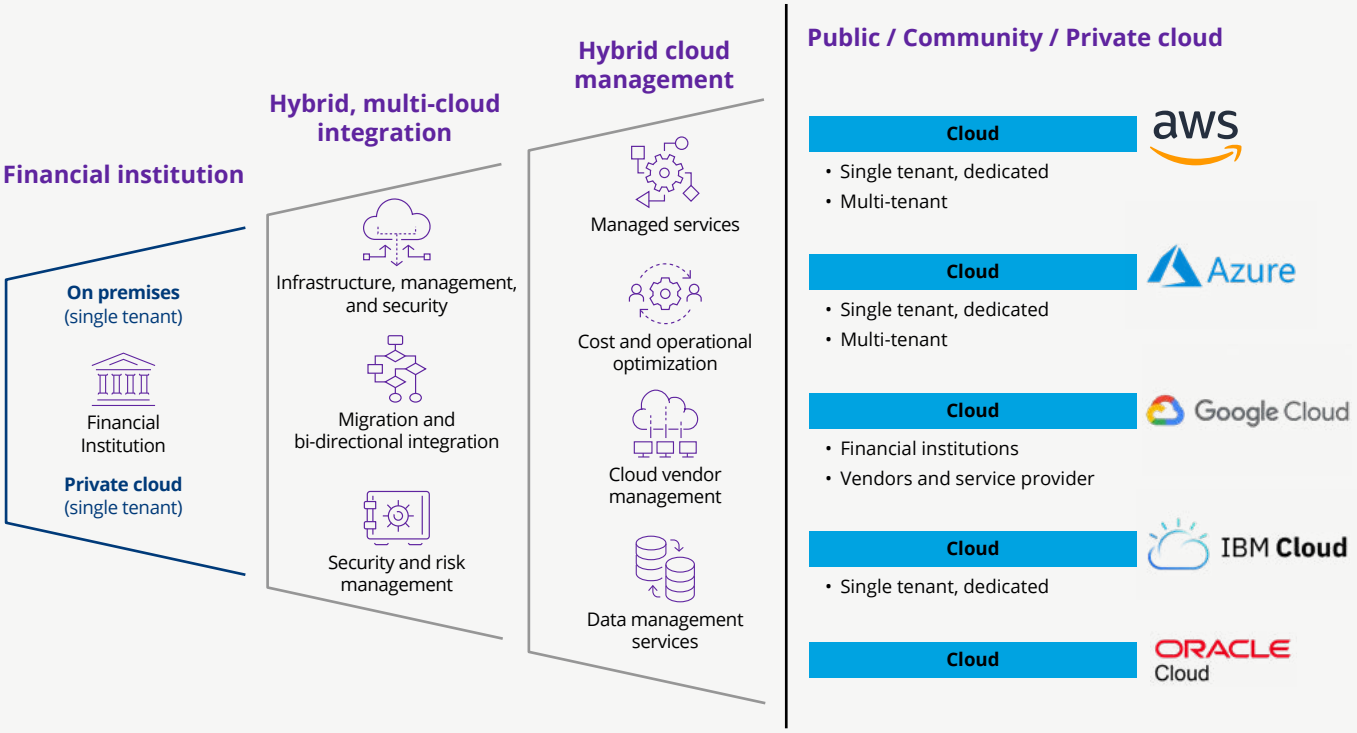
Banking workloads fluctuate with market conditions, customer behavior and transaction volumes. Mainframes are ideal for scaling up to meet peak demands without compromising performance. And when integrated with hybrid cloud services, the scalability becomes even more remarkable.

The hybrid model allows banks to leverage cloud resources for less critical, variable workloads while keeping core, high-volume transactions on the mainframe. This blend of on-prem high-performance and cloud flexibility is perfect for banks rapidly responding to fluctuating markets.

In addition, banks seeking to grow through mergers and acquisitions have the assurance of scalability. Many that have adopted Hogan (running on the IBM Z mainframe) have been among the world's fastest-growing banks.

Banking architecture takes in both hybrid cloud and multi-cloud

(Hybrid cloud blends different types of clouds. Multi-cloud blends different clouds of the same type.)



Source: Celent: Improving Operational Excellence While Migrating to a Hybrid Cloud, Multi-Cloud World – Report 2023

Mainframe hybrid cloud offers a streamlined solution to simplify IT management. The centralized nature of mainframes makes them easier to manage and secure. At the same time, cloud integration provides the flexibility to deploy new services more rapidly.

Banks need simplicity and ease of management to be able to focus more on their core business and less on complicated technological issues.

Let's talk

Can you afford to stand by while quantum competitors snap up IP, talent and ecosystem relationships? It might be a long and winding road to the final destination, but others are speeding past several crucial milestones. Clearly, early adopters will build a tremendous lead and lasting advantage.

To learn more about what it takes to become quantum cybersecure and how Hogan-powered mainframe hybrid cloud enablement can help you become a quantum contender, taking care of securing BAU as well as helping to prepare for future threats and opportunities, visit the **Hogan x page**. Or, if you have a specific issue you'd like to discuss, **contact our experts**.

About **the author**

Duncan Alexander
Product Director, Core Banking

Duncan leads several new and existing core banking products and services within Luxoft's Global Banking Division. He has over three decades of experience applying business technology to achieve strategic goals across multiple industries, including banking, insurance, retail, travel and logistics. Duncan has provided strategic advisory services and delivered mission-critical systems as a strategic partner to clients and has held senior positions in several large enterprises. His primary focus is realizing the business benefits of digital transformation.

About Luxoft

Luxoft, a DXC Technology Company, is a trusted partner in global digital transformation and a leader in delivering competitive advantage in the software-defined world. We engineer and deliver innovative services and products that shape the future of industries by leveraging our extensive partnership network and deep industry-specific expertise.

For more information, please visit **luxoft.com**