

F R O S T & S U L L I V A N

2024 COMPANY OF THE YEAR

*IN THE GLOBAL
POST-QUANTUM
CRYPTOGRAPHY
INDUSTRY*



F R O S T & S U L L I V A N

BEST
2024 PRACTICES
AWARD

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. IBM excels in many of the criteria in the Post-Quantum Cryptography space.

AWARD CRITERIA	
<i>Visionary Innovation & Performance</i>	<i>Customer Impact</i>
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Mega Trends	Customer Purchase Experience
Implementation of Best Practices	Customer Ownership Experience
Leadership Focus	Customer Service Experience
Financial Performance	Brand Equity

Past Expertise Driving Future Capabilities

IBM’s involvement in cryptography dates back to the 1960s when its submission of the Lucifer cipher was adopted as the precursor for Data Encryption Standard (DES). This was the start of a long history of contributions to cryptography and standards, helping to secure modern communications and digital operations. The company’s extensive research in cryptography, its contribution to open-source libraries, and its work at international standards organizations gave it a great advantage in implementing and evaluating the adoption of new algorithms. In 2022, the US National Institute of Standards and Technology (NIST) selected four algorithms from its post-quantum cryptography (PQC) algorithm selection processes to be standardized. IBM researchers, industry, and academia collaborators developed three algorithms: CRYSTALS-Kyber for key exchange, CRYSTALS-Dilithium, and Falcon for digital signatures. NIST will shortly publish two of these algorithms as standards ML-KEM (formerly CRYSTALS-KYBER), and ML-DSA (CRYSTAL-Dilithium). IBM continues to support NIST by submitting three additional quantum-safe signature schemes to its ongoing standardization efforts. Complementing its expertise in quantum computing, the early implementation of quantum-resistant algorithms in its own Cloud, storage, and mainframe products allowed IBM to develop a distinct set of technology capabilities and a competitive advantage in PQC.

“As part of its foundational work on PQC, IBM closely studied over 25 industries and sectors to map out the specific use cases of public key encryption across business value chains. From banking and finance to retail, consumer goods, energy, utilities, telecommunications, and government, the company identified individual dependencies and the impact the transition will have on business processes and operational stages.”

- Özgün Pelit
Sr. Industry Analyst

Moreover, IBM has been instrumental in defining data representation to describe, inventory, and share information about the presence of cryptographic artifacts in applications and systems. A Cryptography Bill of Materials (CBOM) is an extension of the Software Bill of Material (SBOM), a key building block of software security and supply chain risk management. CBOM captures cryptography artifacts and assesses the cryptographic posture of assets. The CBOM concept has been integrated in SBOM standards and is being picked up by vendors, alliances, and open-source projects.

In organizations’ journey to quantum-safe, IBM positions itself as a strategic partner, providing wide-ranging offerings in advisory, consulting, and system integration. The company offers technology for cryptography asset discovery, observability, remediation, crypto-agility solutions, and PQC-

specific education programs. As part of its foundational work on PQC, IBM closely studied over 25 industries and sectors to map out the specific use cases of public key encryption across business value chains. From banking and finance to retail, consumer goods, energy, utilities, telecommunications, and government, the company identified individual dependencies and the impact the transition will have on business processes and operational stages.

IBM offers many cryptography solutions, including cloud key management, certificate lifecycle automation, and managed encryption services. Newer technologies, assets, and methodologies designed to support clients’ PQC journeys are designed and delivered under the “IBM Quantum Safe”. These assets and methodologies have allowed early adopting organizations to test quantum-resistant algorithms in their environments to understand how they will behave in inherently heterogeneous architectures requiring multiple layers of support and expertise. IBM’s other work in the area includes lattice-based cryptosystems, distributed cryptography, homomorphic encryption, and zero-knowledge proofs.

Preparing for the Transformation

In assisting organizations in preparing a roadmap to PQC, IBM employs a comprehensive and cooperative strategy with clients to understand risks, develop transformation blueprints, build foundations, and execute workstreams. This practical strategy involves identifying the network of dependencies and bringing direct and actionable insights aligned with their business criticality. Field-tested and fine-tuned through lessons learned, the transformation framework consists of four steps: developing a quantum-safe heatmap and strategy; discovery, scanning, and inventory; minimum viable product (MVP) and sandbox testing; and insights-driven prioritization and adoption strategy.

In building organizations’ quantum-safe heatmap and strategy, IBM first works with clients to assess the level of complexity of their migration and their data classification specifications. Within the discovery and inventory processes, IBM tools analyze the cryptographic risk in application software code applications and the organizations’ network, infrastructure, and operational environments; this is then correlated with data classifications. IBM Quantum Safe Explorer simplifies this process by scanning all cryptographically

relevant artifacts, surfacing application vulnerabilities, and generating a Cryptography Bill of Materials (CBOM). To provide enterprise-wide visibility, the company's inventory tool, IBM Quantum Safe Advisor, maintains the types and locations of cryptographic instances, assets, data flows, and potential vulnerabilities to ensure quantum-safe cryptographic posture based on business compliance and regulation mandates. Complementing discovery and visibility, IBM Quantum Safe Remediator and assets provide patterns for quantum-safe network communications, container service mesh deployments, and crypto agile applications.

“Approaching PQC beyond merely a technical issue, IBM co-executes transformation plans with clients in an all-encompassing manner. This includes vendor and technology relationship management, training programs, building policies and standards, knowledge management, portfolio optimization, and innovation vehicles for future adaptability.

- Özgün Pelit
Sr. Industry Analyst

In helping clients execute their tailored transformation plan, IBM operates under the established model called the Quantum-Safe Center of Excellence. Approaching PQC beyond merely a technical issue, IBM co-executes transformation plans with clients in an all-encompassing manner. This includes vendor and technology relationship management, training programs, building policies and standards, knowledge management, portfolio optimization, and innovation vehicles for future adaptability. In setting up and scaling such capabilities, IBM's cross-functional teams work hand-in-hand with client teams to ensure consistency, standardization, and establishment of best practices.

Thought Leadership and Collaboration

Beyond its proven enterprise-focused methodology, IBM has also worked with several national governments on PQC. The company helps governments define national quantum-safe advisories and directives at the national level and industry-specific guidelines for critical infrastructure use cases within a country. The IBM team studies and benchmarks different national states' progress and maturity levels on PQC and provides this knowledge to guide best-of-breed government strategies.

IBM has demonstrated thought leadership through multiple initiatives and alliances. This includes leading technical working groups with NIST and other PQC coalitions. IBM also has close engagements with international and regional telecommunications and financial services industry and standards bodies on the definition, implementation, and interoperability of standards. IBM has performed several technical flagship projects with standards entities, industry bodies, and anchor clients.

Conclusion

For enterprises and governments, migration to PQC will be a large-scale undertaking, requiring diverse capabilities and a good understanding of individual operational environments. Far from a one-size-fits-all approach, each organization's transition will be unique, depending on existing capabilities, requirements, risks, and priorities. Combining its expertise in quantum computing and cryptography, IBM positions itself as an all-encompassing partner for organizations in the preparation and execution of the PQC journey. In doing so, IBM harnesses its proven methodology, lessons learned, and best practices to tailor solutions to the specific needs of its clients. Providing a wide range of capabilities for clients' transformation, IBM's offerings and collaborative approach bring clear and targeted outcomes to multiple business units within organizations.

For its strong overall performance, IBM is recognized with Frost & Sullivan's 2024 Global Company of the Year Award in the Post-Quantum Cryptography industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Award is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Award Analysis

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed by a robust solution development process

Visionary Scenarios Through Mega Trends: Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first-to-market solutions and new growth opportunities

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate a consistent and repeatable level of success

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at <http://www.frost.com>.

The Growth Pipeline Engine™

Frost & Sullivan’s proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

[Learn more.](#)

Key Impacts:

- **Growth Pipeline:** Continuous Flow of Growth Opportunities
- **Growth Strategies:** Proven Best Practices
- **Innovation Culture:** Optimized Customer Experience
- **ROI & Margin:** Implementation Excellence
- **Transformational Growth:** Industry Leadership



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- **Mega Trend (MT)**
- **Business Model (BM)**
- **Technology (TE)**
- **Industries (IN)**
- **Customer (CU)**
- **Geographies (GE)**

