



QUANTUM-READY

CRYPTOGRAPHIC ASSET INVENTORY

PREPARED FOR:

ACME FINANCIAL SERVICES

PREPARED BY:

**INTRUVENT
TECHNOLOGIES**

Contact@intruvent.com

Executive Summary

Intruvent Technologies conducted a comprehensive post-quantum cryptography assessment for **Acme Financial Services** between January 6 and January 24, 2025. This assessment identified critical vulnerabilities in the organization's cryptographic infrastructure that may be susceptible to quantum computing attacks within the next 3-5 years. Through a methodical interview and documentation review process, our team documented 127 cryptographic implementations across the enterprise, with 43% utilizing algorithms that are highly vulnerable to quantum computing attacks.

Key Findings

Cryptographic Inventory

- **Identified 127 unique cryptographic implementations** across enterprise systems
- **68% of critical business applications** rely on vulnerable asymmetric encryption algorithms
- **92% of data-at-rest protection** meets current industry standards but lacks quantum resistance
- **14 distinct certificate authorities** manage the organization's PKI infrastructure
- **47 third-party integrations** with varying cryptographic security standards were identified

Risk Assessment

- **43% of cryptographic assets** utilize algorithms with high vulnerability to quantum attacks
- **72% of customer data** is protected by cryptography that requires transition
- **8 critical business functions** depend on cryptographic systems requiring urgent remediation
- **12 regulatory compliance requirements** may be impacted by quantum computing advances
- **\$4.2M estimated financial impact** from a cryptographic failure in core transaction systems

Transition Priorities

- **16 systems** identified for immediate remediation (Phase 1)
- **32 systems** recommended for transition within 12-18 months (Phase 2)
- **79 systems** eligible for standard replacement cycle (Phase 3)

RISK DISTRIBUTION BY ALGORITHM

Algorithm Type	Asset Count	Critical Assets	Risk Level	Common Applications
RSA-2048	42	14	High	TLS Certificates, Document Signing
Diffie-Hellman (< 2048-bit)	27	8	High	VPN Tunnels, Key Exchange
ECDSA P-256	23	9	High	Digital Signatures, Authentication
SHA-1	18	5	Medium	Legacy Applications, Code Signing
DSA (1024-bit)	12	3	High	Legacy Authentication Systems
AES-256	35	12	Low	Data Encryption, Secure Storage
RSA-4096	14	2	Medium	High-Security Communications
ECDHE	19	7	High	Forward Secrecy in TLS

Recommended Next Steps

1. **Implement governance framework** for cryptographic transition with clear accountability
2. **Deploy quantum-resistant standards** for all new implementations and acquisitions
3. **Initiate Phase 1 remediation** for 16 critical systems within 90 days
4. **Create key management transition strategy** for centralized oversight

REPORT CONTINUES...