A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Post-Quantum Cryptography Readiness

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner's Post-Quantum Cryptography Readiness service enables organisations to assess, prepare for, and implement quantum-safe cryptographic solutions. Gartner helps clients identify cryptographic risks, build inventories, and develop tailored migration plans to ensure ongoing data protection and regulatory compliance in the era of quantum computing.

Service Description

Gartner's Post-Quantum Cryptography Readiness service provides a structured and objective approach to help organisations navigate the transition to quantum-safe cryptography. Gartner begins by engaging stakeholders and conducting a comprehensive cryptographic discovery exercise, identifying systems and assets that rely on public key cryptography and evaluating their risk exposure to quantum threats.

Gartner then supports clients in building a detailed inventory of cryptographic assets, assessing application-specific risks, and prioritising remediation activities. Our experts facilitate vendor readiness assessments, ensuring third-party solutions meet post-quantum standards, and help clients develop policies for crypto-agility to enable rapid adoption of new algorithms as they become available. Gartner also provides guidance on regulatory compliance, data retention policies, and the implementation of quantum-safe algorithms, such as ML-KEM and ML-DSA, across critical systems.

Throughout the engagement, Gartner leverages industry best practices, research insights, and frameworks to develop a tailored mitigation plan and migration roadmap. We support operationalisation through training, awareness programmes, and the creation of actionable playbooks, ensuring the organisation is fully prepared for the quantum era and able to maintain secure communication channels and regulatory compliance.

Service Benefits

- Reduces risk of data compromise from quantum-enabled attacks
- Ensures compliance with emerging post-quantum regulations
- Enables rapid adoption of quantum-safe cryptographic algorithms
- Enhances organisational resilience to future cryptographic threats
- Provides clear guidance and best-practice frameworks
- Facilitates stakeholder alignment and informed decision-making
- Improves visibility of cryptographic assets and vulnerabilities
- Strengthens vendor and third-party cryptography assurance
- Accelerates delivery of actionable insights through proven analytical capabilities
- Increases organisational awareness through actionable training programmes

Service Features

- Comprehensive cryptographic discovery and inventory
- Application-specific risk assessment and prioritisation
- Vendor post-quantum readiness assessment
- AI-powered analysis that augments Gartner's Insights and SME delivery experience
- Guidance on quantum-safe algorithm implementation

Gartner®

- Regulatory compliance and risk management support
- Data retention policy review and recommendations
- Migration roadmap and mitigation plan development
- Training and awareness sessions for staff
- Creation of actionable playbooks for operationalisation

Full List of Service Features

- Cryptographic Discovery — Gartner will facilitate workshops to identify all systems, applications, and assets utilising public key cryptography, building a comprehensive inventory and metadata database
- Cryptographic Risk Assessment — Using industry frameworks, Gartner will assess the risk exposure of each cryptographic asset, prioritising remediation based on data sensitivity, business impact, and regulatory requirements
- Vendor Readiness Assessment — Gartner will evaluate third-party and vendor solutions for post-quantum readiness, applying defined assessment criteria and addressing gaps as needed
- Policy and Standards Development — Gartner will help clients create and manage policies for crypto-agility, ensuring applications can rapidly adopt vetted quantum-safe algorithms
- Regulatory Compliance Review — Gartner will provide insight into evolving PQC regulations and standards, supporting clients in achieving and maintaining compliance
- Post Quantum Cryptography Implementation Roadmap — Gartner will develop a tailored migration plan, detailing the transition to quantum-safe algorithms, such as ML-KEM and ML-DSA, and recommending compensating controls where necessary
- Post Quantum Cryptography Training and Awareness — Gartner will deliver targeted training and awareness programmes, equipping staff to support and sustain the post-quantum cryptography transformation

Project Approach

- Week 0: Project Initiation and stakeholder alignment. Gartner will engage with key stakeholders to clarify objectives, define roles, and establish project milestones
- Weeks 1-12: Cryptographic Discovery & Inventory. Gartner will facilitate workshops to identify and document all cryptographic assets and their associated metadata
- Weeks 1-12: Risk Assessment & Prioritisation. Gartner will assess the risk exposure of inventoried assets and prioritise remediation activities based on business impact and regulatory requirements
- Weeks 1-8: Vendor Readiness Assessment. Gartner will evaluate third-party and vendor solutions for post-quantum readiness, identifying gaps and recommending improvements
- Weeks 1-8: Policy Development & Compliance Review. Gartner will support the creation of crypto-agility policies and review data retention and regulatory requirements
- Weeks 1-12: Migration Roadmap & Mitigation Planning. Gartner will develop a detailed plan for transitioning to quantum-safe algorithms and implementing compensating controls

- Weeks 1-12+: Training, Awareness, & Operationalisation. Gartner will deliver training sessions, develop playbooks, and support the operationalisation of the post-quantum cryptography programme

Project Schedule

Gartner anticipates that the Post-Quantum Cryptography Readiness engagement will require approximately 1-12 weeks depending on the activities within scope. The precise timeline will be tailored to the scope and specific requirements of each client and may be adjusted to accommodate organisational complexity, stakeholder or regulatory needs.

This service description is based on a twelve-week engagement.