



Post-Quantum Cryptography (PQC) Services

Service Definition

☎ 0845 519 5465

✉ info@axistwelve.com

🌐 www.axistwelve.com

Table of Contents

Introduction	3
Service Summary	3
Target Audience	3
Service Description.....	3
Core Service Offerings.....	3
<i>PQC Discovery and Assessment Service</i>	3
<i>PQC Migration Planning Service</i>	4
<i>PQC Implementation Service</i>	4
<i>PQC Advisory and Assurance Service</i>	4
Phase 1: Discovery and Planning.....	5
Phase 2: Priority Migration.....	5
Phase 3: Full Migration.....	5
Cryptographic Standards.....	5
Compliance and Accreditations	6
Security Cleared Personnel.....	6
Delivery Model.....	6
Engagement Process	6
Response Times.....	6
Quality Assurance	6
Data Handling.....	7
Information Security	7
Additional Costs	7
Onboarding Process	7
Offboarding Process	7
Client Dependencies.....	8
Training Services.....	8
Documentation	8

Introduction

This service definition document describes our Post-Quantum Cryptography (PQC) technology solution, consultancy and migration services offered through the G-Cloud framework. These services are designed to support UK public sector organisations in preparing for and executing their transition to quantum-resistant cryptographic systems in alignment with the National Cyber Security Centre (NCSC) migration timelines.

Service Summary

Our PQC services help organisations protect sensitive data and critical infrastructure against the future threat posed by quantum computers. Powered by the Venari Adaptive Cryptographic Intelligence Platform we deliver end-to-end support covering cryptographic asset discovery, risk assessment, migration planning, implementation, and ongoing assurance—aligned with NCSC guidance, NIST PQC standards or internal policies.

Target Audience

This service is designed for public sector organisations:

- Central government departments and agencies
- Local authorities
- Blue-light services
- NHS trusts and healthcare organisations
- Critical National Infrastructure (CNI) operators
- Arm's-length bodies and British overseas territories
- Defence and security organisations requiring quantum-safe solutions

Service Description

Core Service Offerings

PQC Discovery and Assessment Service

A comprehensive assessment service to identify cryptographic dependencies across your organisation's networked IT estate, including:

- Full cryptographic inventory and discovery across systems, applications, and infrastructure
- Identification of public key cryptography usage vulnerable to quantum attack
- Assessment of data sensitivity and longevity requirements
- Evaluation of third-party and supply chain cryptographic dependencies
- Classification of assets by migration priority and complexity
- Gap analysis against NCSC PQC migration requirements

Deliverables:

- Cryptographic Asset Register with Cryptographic Bill of Materials (CBOM)
- Risk Assessment Report
- Priority Classification Matrix
- Executive Summary with key findings and recommendations

PQC Migration Planning Service

Strategic planning service to develop a comprehensive roadmap for your organisation's PQC migration:

- Definition of migration goals aligned with organisational objectives
- Development of phased migration strategy aligned to NCSC timelines (2028/2031/2035)
- Identification of highest-priority systems for early migration
- Resource and budget planning across investment cycles
- Supplier engagement and application dependency mapping
- Integration with existing cyber security governance frameworks
- Risk mitigation strategies for systems that cannot be upgraded

Deliverables:

- PQC Migration Strategy Document
- Phased Implementation Roadmap
- Resource and Investment Plan
- Supplier Engagement Framework
- Risk Mitigation Plan

PQC Implementation Service

Technical implementation support for deploying quantum-resistant cryptographic solutions:

- Implementation of NIST-standardised PQC algorithms (ML-KEM, ML-DSA, SLH-DSA)
- Hybrid cryptographic solution deployment (combining classical and PQC)
- Certificate and PKI migration to PQC-compatible standards
- Hardware Security Module (HSM) upgrades and configuration
- Secure key management implementation
- Integration testing and validation
- Configuration of crypto-agile architectures

Deliverables:

- Technical Design Documentation
- Implementation Runbooks
- Test Reports and Validation Certificates
- Updated Security Architecture Documentation
- Operational Handover Documentation

PQC Advisory and Assurance Service

Ongoing advisory support and assurance services:

- Expert guidance on PQC adoption and standards evolution
- Security architecture reviews with PQC considerations
- Compliance assessment against NCSC guidance
- Supply chain security assessment for PQC readiness
- Periodic review and roadmap updates
- Board-level briefings and awareness sessions
- Training and capability building for technical teams

Deliverables:

- Advisory Reports
- Compliance Assessment Reports

- Training Materials and Workshop Delivery
- Quarterly Progress Reviews

Alignment with NCSC PQC Migration Timeline

Our services are structured to support organisations through each phase of the NCSC migration timeline:

Phase 1: Discovery and Planning

Objective: Complete discovery, assessment, and initial migration planning

Our Support:

- Cryptographic asset discovery and inventory services
- Risk assessment and prioritisation
- Development of initial migration plans
- Supplier communication and engagement support
- Investment case development

Phase 2: Priority Migration

Objective: Execute high-priority migrations and refine plans

Our Support:

- Implementation of PQC for highest-priority systems
- Infrastructure preparation for PQC
- Plan refinement based on ecosystem developments
- Continued advisory and assurance services

Phase 3: Full Migration

Objective: Complete migration across all systems

Our Support:

- Full implementation across remaining systems
- Legacy system migration or retirement
- Enhanced cyber resilience integration
- Final validation and assurance

Technical Standards and Compliance

Cryptographic Standards

Our services implement and support the following NIST-standardised PQC algorithms:

- ML-KEM (FIPS 203): Module-Lattice-Based Key Encapsulation Mechanism for secure key exchange
- ML-DSA (FIPS 204): Module-Lattice-Based Digital Signature Algorithm for authentication
- SLH-DSA (FIPS 205): Stateless Hash-Based Digital Signature Algorithm

Algorithm evolution is closely monitored, and support for revised standards e.g. FIPS 205 is delivered in a timely manner.

Compliance and Accreditations

- Aligned with NCSC Post-Quantum Cryptography guidance
- Support for FIPS 140-3 validated implementations
- Cyber Essentials Plus certified organisation
- ISO 27001 certified Information Security Management System
- NCSC Assured Cyber Security Consultancy (ACSC) scheme alignment
- Support for compliance with sector-specific regulations (FCA, NHS DSPT, etc.)

Security Cleared Personnel

Our consultants hold appropriate security clearances for working with government and CNI organisations, including SC and DV clearances as required.

Service Delivery

Delivery Model

Services are delivered through a combination of:

- Active and passive sensors deployed at client premises and in 'cloud' environments
- On-site consultancy at client premises (UK-wide)
- Remote delivery via secure collaboration platforms
- Hybrid delivery models as appropriate

Engagement Process

1. Initial Consultation: Scoping discussion to understand requirements
2. Proposal: Detailed proposal with scope, timeline, and costs
3. Kick-off: Project initiation and governance establishment
4. Delivery: Phased delivery with regular checkpoints
5. Handover: Documentation and knowledge transfer
6. Follow-up: Optional ongoing advisory support

Response Times

Priority	Description	Initial Response
Critical	Service-affecting security incident	2 hours
High	Urgent advisory requirement	4 hours
Medium	Standard service request	1 business day
Low	General enquiry	3 business days

Quality Assurance

- All deliverables subject to peer review
- Named engagement lead for accountability
- Regular progress reporting against milestones

- Client satisfaction surveys at engagement conclusion

Data Protection and Security

Data Handling

- All client data processed in accordance with UK GDPR and Data Protection Act 2018
- Data processed and stored within the UK only (when required)
- Secure deletion of client data upon engagement completion (unless retention required)
- Encrypted transmission and storage of sensitive information

Information Security

- ISO 27001 certified information security management
- Regular security assessments and penetration testing
- Security cleared personnel for classified work
- Secure collaboration tools approved for government use

Additional Costs

- Travel and expenses charged at cost where on-site delivery is required outside standard locations
- Out-of-hours working charged at premium rates as specified in pricing document
- No hidden fees or additional charges beyond agreed scope9. Onboarding and Offboarding

Onboarding Process

1. Contract execution and purchase order receipt
2. Security clearance verification and vetting (if required)
3. Access provisioning and account setup
4. Project kick-off and governance establishment
5. Knowledge transfer and context briefing
6. Commencement of service delivery

Typical onboarding timeline: 2-4 weeks depending on security clearance requirements

Offboarding Process

1. Final deliverable handover and sign-off
2. Knowledge transfer to client teams
3. Documentation of all work completed
4. Secure return or deletion of client data
5. Access revocation and account closure
6. Post-engagement review and feedback

Data portability: All deliverables provided in standard, portable formats (PDF, DOCX, XLSX, JSON standard data formats as appropriate)

Dependencies and Constraints

Client Dependencies

Successful delivery requires:

- Timely provision of access to systems and information including deployment of active and passive sensors (where required)
- Availability of client stakeholders for workshops and reviews
- Timely decision-making and approvals
- Completion of any prerequisite security clearances

Training Services

- Executive briefings on quantum threat and PQC
- Technical training on PQC algorithms and implementation
- Operational training for security teams
- Awareness sessions for broader IT teams

Documentation

All engagements include comprehensive documentation:

- Technical documentation
- Process and procedure guides
- Training materials
- Executive summaries¹². Subcontractors and Partners

We may utilise specialist subcontractors for specific technical requirements. Any subcontractors:

- Are vetted to equivalent security standards
- Hold appropriate security clearances
- Are disclosed to clients prior to engagement
- Operate under equivalent contractual obligation