THALES
Building a future we can all trust

G-Cloud 15

PQC DISCOVERY AND ASSESSMENT

Doc Ref No: ThalesGC1501

INTRODUCTION

Prepare your organisation for the quantum computing era with structured, risk-based migration to quantum-safe cryptography.

The Post-Quantum Cryptography (PQC) Transition Consultancy is a comprehensive advisory and assessment service designed to help organisations systematically plan, assess, and execute migration from classical cryptographic algorithms to quantum-safe alternatives. Aligned with ETSI TR 104 106, we deliver evidence-based prioritisation, realistic migration roadmaps, and executable implementation plans that address real-world constraints including supply chain dependencies, regulatory requirements, and budget limitations.

USE CASE

Government departments, defence contractors, critical national infrastructure operators, and organisations handling sensitive data face an urgent challenge: the threat of "harvest now, decrypt later" attacks means migration planning must begin immediately, even though full quantum computer capability may be years away.

NCSC mandates critical asset migration by 2031 and full migration by 2035. This consultancy serves organisations that need to understand their quantum computing exposure and develop actionable migration strategies before regulatory deadlines and competitive pressures intensify.

SERVICE DESCRIPTION

Features

Evidence-Based Risk Assessment: Comprehensive vulnerability analysis using the CARAF framework with quantitative risk scoring (1-4 scale). Prioritisation driven by actual exposure rather than arbitrary timelines.

Comprehensive Asset Discovery: Top-down security architecture assessment identifying cryptographic assets, cryptographically-protected assets, implementation dependencies, and trust dependencies across your entire estate.

Dependency Intelligence: Detailed mapping of inter-asset dependencies that frequently derail migrations, including third-party vendor constraints, certification requirements, and supply chain considerations.

Multi-Jurisdictional Regulatory Alignment: Guidance accounting for divergent requirements across UK (NCSC), EU, US (NIST), and other national frameworks including hybrid approach considerations for French, Chinese, and Korean markets.

Solution Architecture: Specific cryptographic algorithm recommendations with migration approach selection (pure, parallel, or backward-compatible) tailored to each asset class and operational context.

Crypto Agility Design: Forward-looking architecture recommendations that prevent future cryptographic transitions from being equally costly and disruptive.

Certification Impact Assessment: Analysis of re-certification requirements for Common Criteria, FIPS, and other security certifications affected by algorithm changes.

Benefits

Risk Reduction: Clear quantification of quantum computing exposure with measurable before and after metrics, enabling informed investment decisions and governance reporting.

Resource Efficiency: 30-50% more efficient resource allocation through evidence-based prioritisation, preventing costly "boil the ocean" approaches that attempt to migrate all cryptography simultaneously.

Regulatory Compliance: Proactive alignment with NCSC guidance (2031/2035 deadlines), NIST post-quantum standards, and emerging EU mandates, with documented evidence for audits and governance.

Conflict Prevention: 80%+ of anticipated migration conflicts identified and mitigated during planning phase, reducing costly rework and schedule delays during implementation.

Competitive Advantage: Early quantum-safe capability demonstrating commitment to long-term security, enhancing customer confidence and supply chain resilience.

Timeline Clarity: Specific, realistic migration timelines with confidence intervals, enabling accurate budget planning and stakeholder communication.

DETAILED SERVICE OVERVIEW

The consultancy operates through a structured 5-phase engagement model aligned with PQC Transition Planning methodologies:

Phase 1: Assessment and Scoping

Define PQC transition goals and drivers (regulatory, strategic, operational). Identify scope including deployed products, supporting systems, development environments, and third-party dependencies. Establish governance and stakeholder alignment.

Output: Scoped assessment plan with clear boundaries and success criteria.

Phase 2: Inventory and Dependency Analysis

Conduct top-down security architecture assessment. Identify cryptographic assets and cryptographically-protected assets. Document implementation dependencies and trust dependencies. Map external interoperability constraints and third-party dependencies.

Output: Comprehensive asset inventory and dependency mapping document.

Phase 3: Vulnerability and Risk Assessment

Analyse quantum computing vulnerability for each cryptographic asset. Perform risk assessment considering likelihood and impact of CRQC-enabled attacks. Identify assets requiring immediate attention versus lower-priority migrations.

Output: Detailed vulnerability and risk assessment report with quantified prioritisation.

Phase 4: Solution Selection and Planning

Identify candidate quantum-safe solutions for each vulnerable asset. Evaluate solutions against technical requirements and constraints. Perform cost/benefit analysis and implementation feasibility assessment. Define migration approaches (pure, parallel, backward-compatible).

Output: Technical solution specifications and preliminary migration strategy.

Phase 5: Roadmap Development and Execution Planning

Reconcile dependencies and identify migration conflicts. Develop phased migration roadmap with realistic sequencing. Create detailed execution plans including resource requirements, timeline and milestone planning, risk mitigation strategies, governance framework, and vendor engagement approach.

Output: Comprehensive quantum-safe migration roadmap and execution blueprint.

Engagement Variants

Product Focused: For product security teams assessing PQC readiness of manufactured products, supporting infrastructure, and supply chain dependencies. Focuses on product architecture, lifecycle management, and third-party component strategies.

Enterprise Focused: For large organisations with complex IT infrastructure, multiple business units, and diverse technology stacks. Addresses enterprise-wide dependencies, phased rollout strategies, and business continuity considerations.

Critical Infrastructure: For organisations operating critical systems with strict certification and regulatory requirements. Incorporates regulatory compliance pathways, security certification considerations, and cross-organisational coordination needs.

Typical Deliverables

Assessment Report: Executive summary, detailed vulnerability analysis, risk quantification, and mitigation recommendations.

Asset Inventory Document: Comprehensive catalogue, dependency mapping, trust dependency analysis, and interoperability constraints.

Migration Strategy Document: Solution assessment, algorithm recommendations, and migration approach selection.

Quantum-Safe Roadmap: Phased migration plan, resource requirements, conflict resolution, and vendor engagement approach.

Execution Blueprint: Implementation procedures, governance framework, milestones, and success metrics.

ABOUT THALES

Thales in the UK has been harnessing technology to benefit the nation for over a century. Across all walks of life, you will find us securing and protecting every moment. We develop world-leading capabilities to help our customers think smarter and act faster.

Thales collaborate with partners in both government and industry, providing cutting-edge technologies to the civil and defence markets.

Thales has a significant presence across the UK, with locations strategically positioned in England, Wales, Northern Ireland, and Scotland. This geographic reach enables us to effectively support the diverse needs of local communities while contributing to the economic prosperity of all four nations. Our key facilities, along with several customer-facing sites, extend from the South West of England to Glasgow, reinforcing our commitment to regional investment and development.

The most trusted organisations in the world rely on Thales for cybersecurity solutions that keep critical assets safe. With more than 6,000 cybersecurity experts worldwide, our portfolio protects applications, data and identities, including services that close compliance gaps, detect and monitor threats and strengthen defences.

For further information, please see https://www.thalesgroup.com/en/worldwide/united-kingdom