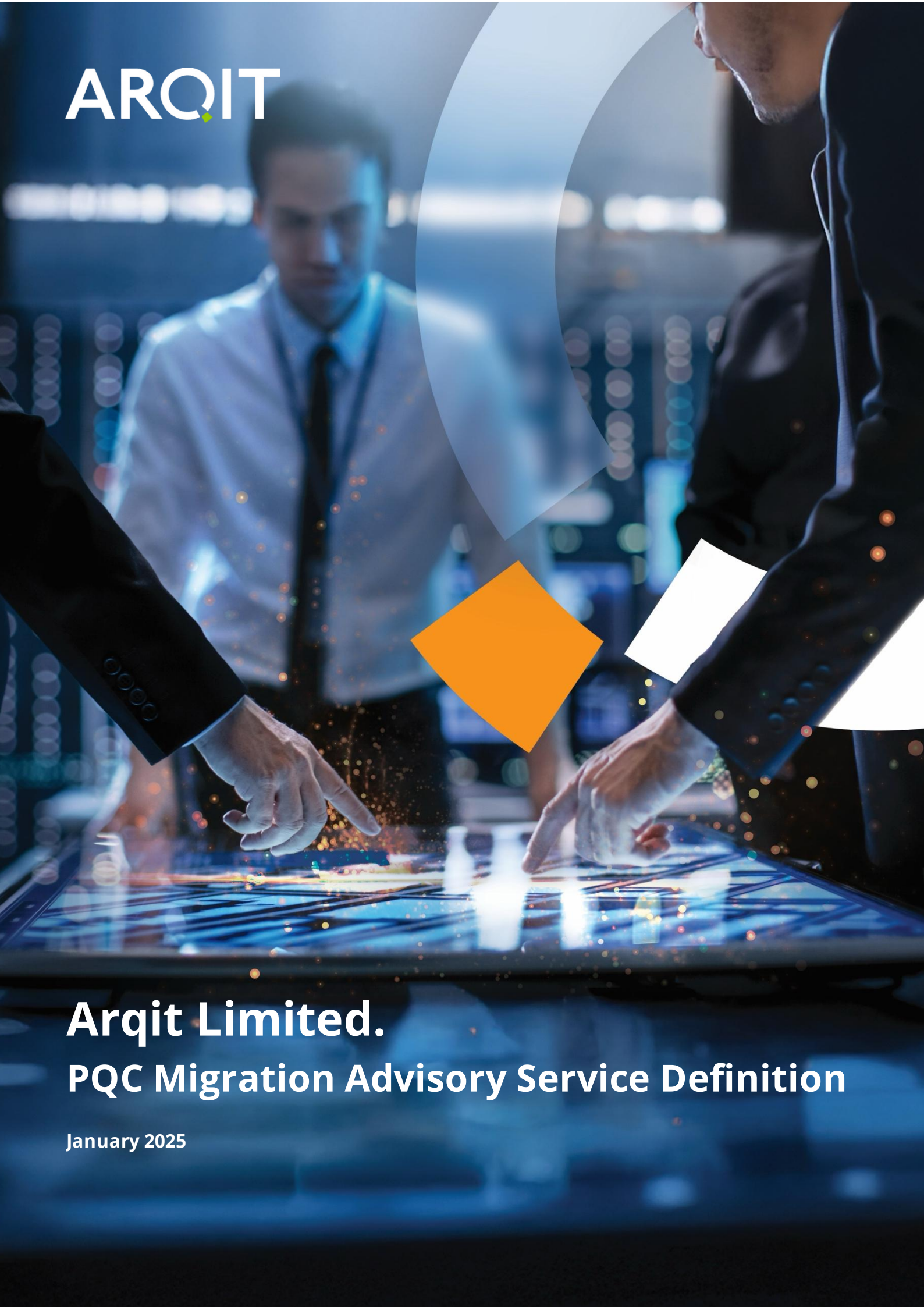

Arqit Limited.

PQC Migration Advisory Service Definition

January 2025

Introduction

The Importance of Encryption

Cyber security breaches continue to grow in number and severity across all industries and all types of organisations. The business risk of cyber security attack grows constantly and can pose an existential threat to any organisation.

At the same time, the sophistication of attacks is constantly increasing, with multi-national 'professional' threat actors (including those backed by nation states) growing and ramping up their activities. The risk that organisation data could be stolen or compromised is very real and the impact is likely to be catastrophic.

Encryption of data is at the core of most protection strategies – effective encryption of communications prevents threat actors from eavesdropping data or impersonating a legitimate business contact; and data which is encrypted properly will be safe even if the underlying system or communications path is otherwise compromised.

In recent years, the commercial and operational model of Cloud services has resulted in a near-universal movement to Cloud delivery on the part of enterprise application vendors. In-house applications have been shifted out of the office and into public Cloud infrastructure (virtual private cloud, VPC). Enterprise software applications are now routinely delivered from the Cloud on a Software-as-a-Service (SaaS) model.

With Cloud, the issues of data protection become even more important, as large amounts of potentially critical sensitive data flow out of the logical perimeter of the organisation and into the purview of the application vendor. It becomes necessary to understand and assess the security posture of every SaaS vendor and Cloud platform, since they have become part of the supply chain and extended operations of the organisation. Identifying and approving all vendors in the supply chain is a critical element of Information Security certification such as ISO 27001.

The Quantum Threat to Encryption

It is now well-established that quantum computers represent a fundamental threat to the most prevalent encryption schemes in use today. As quantum computers continue to advance rapidly, they will become capable of breaking encryption, rendering encrypted data vulnerable to eavesdropping and misuse. The public-private key encryption schemes used by everything from mobile phones to web servers (including SaaS applications) to connected IoT devices and Operational Technology (OT) will be vulnerable.

Although publicly-announced quantum computers have not yet attained a level of capability that would allow state-of-the-art encryption to be attacked successfully, the rate of advancement is rapid. Encryption schemes being deployed today must be assessed for future security given that systems may be in use for many years. Government security agencies around the world, including in the US,UK and EU have warned that

© Copyright Arqit Quantum.Inc 2025

sophisticated threat actors are likely to be storing encrypted data now in order to decrypt it later when more capable quantum computers become available (so-called 'Harvest Now, Decrypt Later' attacks). The mitigation is the migration to quantum-secure communications through "Post Quantum Cryptography". Post-quantum security will be one of the largest and most complex technology transitions of the decade. Those who start early will be the ones who maintain trust, resilience and competitive advantage. Those who delay will face a rushed, expensive and highly disruptive upgrade.

Cryptographic Inventory

Given the importance of encryption to overall security, it is vital that every organisation understands how and where encryption is used within its business. Each organisation must actively investigate all potentially sensitive network communications and make a determination about the level of risk involved.

The UK's National Cyber Security Centre (NCSC) has set out guidance for Post Quantum Migration planning (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines): By 2028 organisations should have carried out a full discovery exercise and built an initial plan for migration of systems to Post- Quantum Cryptography.

Arqit is proud to have been selected to join NCSC's Post-Quantum Cryptography (PQC) migration advice pilot. This is an assured consultancy scheme launched in 2025 to help UK organizations prepare for the quantum threat by certifying experts in PQC discovery, planning, and implementation. It provides vetted consultants for complex cyber needs, helping businesses map crypto assets, prioritize systems, and build roadmaps.

© Copyright Arqit Quantum.Inc 2025

PQC Migration Advisory Service

The PQC Migration Advisory Service provided by Arqit will help you to understand the risks posed to the security of your organisation due to encryption technologies today, and plan for an efficient and effective migration to the latest post-quantum cryptography technologies.

A PQC Migration Advisory activity will be led by our expert consultants, with a deep understanding of the issues relating to encryption deployment, and able to advise on strategies and policies that will ensure your organisation remains secure and compliant with best practice.

PQC Migration Advisory is grounded in Discovery: gathering a current view of encryption usage and hence risks within your organisation, based on actual data collected from your infrastructure. It is not a discussion of theoretical risks based on a typical organisation – it will provide real, relevant, actionable insights for your organisation.

The PQC Migration Advisory service will inform and educate your technical and risk management teams about the current and future risks and issues related to encryption, and the best practices for migration to post-quantum cryptography. Our consultants will hold a series of meetings and workshops to understand background information and to discuss actual findings from the data collection exercise within your organisation, providing insights based on PQC migration engagements with our global client base.

The service will deliver concrete recommendations for management of encryption risk, including a pathway to a standard operating model which encompasses and addresses encryption risk now and into the future. These will help you meet the recommendations of cyber-security agencies such as NCSC (UK), ENISA (EU) and CISA (USA) amongst others, ensuring that you benefit from learnings and best practices of trailblazing adopters of post-quantum encryption technology.

The PQC Migration Advisory service will provide assistance with building plans to understand and address the major risks associated with quantum-computer attacks against current encryption. Our consultants have expertise in current encryption technologies and understand the mechanisms that can be deployed to protect data against quantum attack. We will help you develop an appropriate strategy based on your unique threat landscape, and devise reusable playbooks and tools that can be used across the organisation to carry out encryption discovery and migration to PQC.

Encryption Risk Advisory Service Delivery

The Encryption Risk Advisory Service will be customised for the organisation, but in outline will typically include the following:

Project initiation and definition

Our consultants will work with the technical and risk management teams within your organisation to scope the advisory engagement. This will include engagement with stakeholders to understand your needs and customise the project goals and outcomes to deliver maximum value.

© Copyright Arqit Quantum.Inc 2025

Data Collection Design

Working with your technical team, a data collection exercise will be scoped and planned so that a representative set of data can be collected from your organisation, so that real data-derived insight can be gained.

Data Collection

Using Arqit's Encryption Intelligence data collection and analysis technology, data can be collected from your organisation infrastructure for a period of time (typically several weeks to gain a good spread of data). This data can be analysed by our platform as the basis for PQC Migration Advisory. **Note:** that the Encryption Intelligence product is not included in in this PQC Migration Advisory service, but is available for purchase by the buyer through a separate G-Cloud service (a Lot 2 service called "Encryption Intelligence").

Education and Analysis

Our consultants will carry out extensive offline analysis of data collected from your organisation and develop a view on the overall encryption landscape within the organisation (a comprehensive cryptographic inventory). Note that if the Arqit Encryption Intelligence software product is not deployed, then analysis will be limited to data collected manually and provided to us by the Buyer.

This will include one or more interactive workshops with stakeholders to gather viewpoints and to educate about key aspects of encryption risk – using your own data to illustrate.

Reporting and Recommendations

At the end of the Encryption Risk Advisory process a detailed written report will be produced, including a summary of the encryption risks for the organisation, and recommendations for short- and long-term actions as a result of the findings. This will be presented to stakeholders including senior management sponsors.

© Copyright Arqit Quantum.Inc 2025

Additional Services

Arqit and our partners can provide a series of additional services if these are relevant and required by the buyer. These services are also available through G-Cloud, and our consultants will be happy to discuss these with the buyer at an appropriate time.

These services include (for example):

- Development of detailed encryption security strategies.
- Development and implementation of post-quantum cryptography migration plans.
- Advisory services related to specification, procurement and implementation of quantum-safe applications and infrastructure.
- Ongoing policy-based management of encryption risk, as a self-serve application for your team to use or as a fully managed service.

Registered number: 10544841. Registered Office: 3 Orchard Place, London, England, SW1H 0BF | Proprietary and Confidential

© Copyright Arqit Quantum.Inc 2025

ARQIT

nqa
ISO 27001
INFORMATION SECURITY MANAGEMENT

FIPS 140-3™

A member of ADS

Assured Service Provider
National Cyber Security Centre
Consultancy: Post-Quantum Cryptography (Discovery and Migration Planning)

arqitgroup.com

consultancy@arqit.uk

Arqit

CYBER ESSENTIALS PLUS