



# Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials)

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

**CGI**

# Table of contents

|                              |                                                 |          |
|------------------------------|-------------------------------------------------|----------|
| <b>1.</b>                    | <b>Service Description</b>                      | <b>5</b> |
| 1.1.                         | Are you ready for a quantum disruption?         | 5        |
| 1.2.                         | Overview of the PQC Essentials services         | 6        |
| 1.3.                         | PQC Essentials delivery lifecycle               | 6        |
| 1.4.                         | Cryptographic dependency discovery              | 7        |
| <b>2.</b>                    | <b>Service Continuity</b>                       | <b>7</b> |
| <b>3.</b>                    | <b>Onboarding and Offboarding</b>               | <b>7</b> |
| 3.1.                         | Onboarding                                      | 7        |
| 3.2.                         | Offboarding                                     | 8        |
| <b>4.</b>                    | <b>Service constraints</b>                      | <b>8</b> |
| <b>5.</b>                    | <b>Service levels</b>                           | <b>8</b> |
| <b>6.</b>                    | <b>Hosting options and locations</b>            | <b>8</b> |
| <b>7.</b>                    | <b>Security</b>                                 | <b>8</b> |
| <b>8.</b>                    | <b>Service Pricing and Terms and Conditions</b> | <b>9</b> |
| 8.1.                         | Pricing                                         | 9        |
| 8.2.                         | Terms and Conditions                            | 9        |
| <b>9.</b>                    | <b>Further information</b>                      | <b>9</b> |
| PROPRIETARY AND CONFIDENTIAL |                                                 | 10       |

# Service Definition overview

Organisations increasingly rely on cryptography to protect sensitive information, assure digital services, and maintain trust across complex technology and supply-chain ecosystems. The emergence of cryptographically relevant quantum computing introduces a new class of systemic risk: cryptographic mechanisms that are secure today may become vulnerable in the future, potentially exposing long-lived data and undermining critical services.

Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) supports organisations in understanding, managing, and preparing for this risk in a structured and proportionate manner. The service focuses on identifying where cryptography underpins business-critical services, assessing exposure to quantum-related threats, and developing a clear, prioritised plan for transition to quantum-safe cryptography, while maintaining operational continuity.

PQC Essentials applies proven business continuity, cyber risk, and operational resilience principles to cryptographic risk. It enables organisations to understand the impact of quantum threats on confidentiality, integrity, and availability, and to make informed decisions aligned to business priorities, regulatory expectations, and risk appetite. This includes consideration of data lifetimes, service criticality, third-party dependencies, and the need to maintain uninterrupted service delivery during cryptographic transition.

The service is aligned with UK National Cyber Security Centre (NCSC) guidance on PQC readiness and supports organisations in taking the necessary first steps toward quantum resilience. Outcomes include improved visibility of cryptographic dependencies, a quantified understanding of risk, and a structured migration plan that supports long-term security, resilience, and confidence in the face of emerging quantum threats.

## **CGI's approach:**

CGI's approach to Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) is structured, outcome-driven, and aligned to UK National Cyber Security Centre (NCSC) guidance. It is designed to help organisations take practical, proportionate first steps towards quantum resilience while maintaining continuity of critical services.

CGI recognises that Post-Quantum Cryptography is not a single technology change but a multi-year transformation that impacts business processes, technology architectures, data management, and supply chains. PQC Essentials therefore focuses on building a clear, evidence-based understanding of cryptographic risk and providing a robust foundation for informed decision-making.

Our approach combines deep cryptographic expertise with operational, regulatory, and continuity considerations, enabling organisations to:

- Clearly define the scope, objectives, and stakeholders for PQC transition.
- Understand where cryptography underpins critical business and operational services.
- Assess exposure to quantum-related threats, including long-lived data and third-party dependencies.
- Prioritise action based on business impact, data sensitivity, and risk appetite.

CGI delivers PQC Essentials through a phased model covering scoping, discovery, and migration planning. During discovery, we identify and assess cryptographic assets across IT and operational environments, mapping cryptographic usage, data lifetimes, and supplier dependencies. This enables the development of a prioritised risk view that highlights where quantum threats pose the greatest risk to confidentiality, integrity, or availability.

Building on this understanding, CGI develops a high-level migration strategy and roadmap aligned to organisational priorities and NCSC guidance. This roadmap integrates security risk reduction, regulatory alignment, value for money, and operational continuity considerations, ensuring that quantum-safe transition planning supports ongoing service delivery rather than disrupting it.

Throughout the engagement, CGI applies established governance, assurance, and continuity principles drawn from ISO 22301, ISO 27001, and operational resilience good practice. This ensures PQC Essentials delivers

clear, actionable outcomes that form a strong foundation for subsequent PQC implementation, assurance, and long-term resilience activities.

## Why CGI?

CGI has developed strong expertise in cryptographic modernisation and Post Quantum Cryptography (PQC) readiness through long-term involvement in complex, regulated, and large-scale environments where cryptography is mission critical. Our experience spans safety-critical aerospace systems, national-scale public infrastructure, regulated energy networks, and high-volume IoT platforms, giving CGI a practical and evidence-based understanding of how cryptographic change must be delivered in real-world operational settings.

Across these environments, cryptography underpins trust, safety, and availability. CGI understands the challenges of operating and evolving standard cryptography at scale, including key management, certificate lifecycles, performance constraints, and interoperability across legacy and modern platforms. Building on this foundation, CGI supports organisations in preparing for the transition to quantum-resistant cryptographic standards, ensuring alignment with emerging international standards and UK NCSC guidance.

In parallel, CGI has experience working within environments that require the use of sovereign cryptography, national algorithms, or jurisdiction-specific cryptographic controls. This enables CGI to support organisations with complex assurance, regulatory, and national security requirements, where cryptographic choices must balance compliance, interoperability, and long-term resilience.

CGI's approach to PQC is grounded in operational continuity and risk management. We recognise that PQC transition is not a single technology upgrade, but a phased transformation that affects systems, data lifetimes, supply chains, and service delivery. Our experience allows us to help organisations identify where cryptography is business-critical, assess exposure to quantum-related threats, and plan migration in a way that maintains service availability and confidence.

As an NCSC-assured cyber security consultancy, CGI combines deep cryptographic expertise with strong governance, assurance, and operational resilience capabilities. This enables us to deliver Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) that is practical, proportionate, and tailored to the realities of complex public sector and regulated environments - providing clients with clarity, confidence, and a strong foundation for long-term quantum resilience.

# 1. Service Description

As one of the largest security practices in the UK, CGI has developed deep expertise in cryptographic modernisation and Post Quantum Cryptography (PQC) readiness through more than 40 years of supporting government and commercial organisations operating in highly regulated and mission-critical environments. Our experience spans safety-critical systems, national-scale public infrastructure, regulated energy networks, and high-volume digital platforms, where cryptography is fundamental to trust, resilience, and service continuity.

CGI has invested significantly in the people, capabilities, and infrastructure required to support sensitive Public Sector and Critical National Infrastructure engagements. CGI operates a dedicated Security Directorate, maintaining List X facilities, appropriate security clearances, accredited infrastructure, and trusted interconnections with government networks. CGI's corporate infrastructure is certified to recognised standards including ISO/IEC 27001:2022, and our security and assurance practices align with ISO 22301, NIST, and UK National Cyber Security Centre (NCSC) guidance. This enables CGI consultants to work securely with protectively marked material and apply the same high standards to client environments.

Our cryptography and cyber security specialists hold a broad range of industry-recognised qualifications relevant to Public Sector and regulated environments. This includes expertise across standard cryptography, sovereign cryptographic requirements, and emerging quantum-resistant algorithms, supported by strong assurance, risk, and operational resilience capability. This blend of technical and governance expertise allows CGI to deliver PQC services that are practical, proportionate, and aligned to real-world operational constraints.

Because of these capabilities and experience, CGI provides Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) as a structured, outcome-driven service that can be tailored to an organisation's technical landscape, regulatory obligations, and risk appetite. As one of the leading IT and business consulting providers in the UK, CGI is well placed to support organisations by:

- Scoping PQC discovery activities and developing an initial business case aligned to organisational priorities.
- Identifying cryptographic dependencies across business-critical services, data, and supply chains.
- Assessing exposure to quantum-related threats, including long-lived data and third-party risk.
- Producing a prioritised view of cryptographic risk to support informed decision-making.
- Developing a high-level PQC migration strategy and roadmap aligned to NCSC guidance.
- Advising on interim and transitional cryptographic approaches to maintain service continuity.
- Supporting assurance, governance, and evidence generation to demonstrate due diligence.
- Providing knowledge transfer, briefings, and awareness sessions for technical and senior stakeholders.

CGI's PQC Essentials service provides organisations with clarity, confidence, and a robust foundation for longer-term quantum-safe transformation, while ensuring that critical services remain secure, trusted, and operational throughout the transition.

## 1.1. Are you ready for a quantum disruption?

The advent of cryptographically relevant quantum computing presents a material continuity risk to organisations that rely on classical public-key cryptography to protect sensitive data and critical services. The risk is not theoretical: harvest now, decrypt later attacks mean that data captured today may be compromised in the future once quantum capabilities mature.

PQC Essentials helps organisations discover their cryptographic inventory and develop structured, prioritised plans to migrate to quantum-safe solutions with minimal operational disruption. The service provides clear visibility of where cryptography underpins critical services, data, and supply chains, and supports informed decision-making aligned to business risk, regulatory expectations, and service continuity requirements. This ensures organisations can transition to quantum-resistant cryptography while maintaining confidence, availability, and trust throughout the migration period.

## 1.2. Overview of the PQC Essentials services

CGI's Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) applies proven Business Continuity and Operational Resilience principles to cryptographic risk. It provides a managed, outcome-driven approach to:

- Identify cryptographic dependencies across business-critical services.
- Assess exposure to quantum-related threats.
- Define recovery and transition strategies aligned to NCSC guidance.
- Ensure continuity of operations during PQC migration.

The service is designed for public sector, CNI, defence, health, and regulated industries where long-lived data, availability, and assurance are critical.

## 1.3. PQC Essentials delivery lifecycle

CGI delivers Post Quantum Cryptography Discovery and Migration Planning (PQC Essentials) as a structured, end-to-end journey that addresses immediate cryptographic risk while laying the foundations for long-term quantum-safe transformation. The lifecycle is designed to provide organisations with clarity, evidence, and a prioritised roadmap before committing to large-scale implementation.

The service is structured in two complementary phases.

### Phase 1 - Discovery and exploration

The initial phase focuses on building a clear, evidence-based understanding of cryptographic risk and organisational readiness. This phase enables informed decision-making and supports the development of a robust business case for PQC transition.

Typical activities include:

- Cryptographic scoping and prioritisation.

Definition of scope, stakeholders, and objectives, aligned to business-critical services, regulatory drivers, and risk appetite.

- Cryptographic discovery and inventory development.

Identification of cryptographic assets across prioritised IT and operational environments, including applications, platforms, data flows, and third-party dependencies.

- Data lifetime and quantum risk assessment.

Assessment of data sensitivity, retention periods, and exposure to quantum-related threats, including harvest now, decrypt later risks.

- Risk analysis and impact assessment.

Development of a prioritised view of cryptographic risk, highlighting where quantum threats may impact confidentiality, integrity, availability, or service continuity.

### Outcome:

Clear visibility of cryptographic dependencies, validated priorities, and an evidence-based foundation for migration planning.

### Phase 2 - Migration planning and roadmap development

Building on the outputs of the discovery phase, CGI develops a structured and proportionate plan for transition to quantum-safe cryptography. This phase focuses on how and when migration should occur, without disrupting critical services.

Typical activities include:

- Quantum-safe migration strategy definition.

Development of a high-level migration approach aligned to NCSC guidance, business priorities, and enterprise architecture roadmaps.

- Sequencing and dependency analysis.

Identification of migration waves, interim hybrid-cryptography approaches, and dependencies across systems, services, and suppliers.

- Infrastructure and capability considerations.

Identification of future requirements for cryptographic infrastructure, such as PKI, HSMs, crypto-agility, and key lifecycle management.

- Governance, assurance, and compliance planning.

Definition of policies, controls, and assurance mechanisms to support sustained cryptographic resilience over time.

- Supplier and third-party readiness assessment.

Consideration of vendor alignment, contractual impacts, and ecosystem dependencies affecting PQC transition.

#### **Outcome:**

A prioritised, actionable migration roadmap that supports quantum-safe transition while maintaining operational continuity.

#### **A structured and adaptive path to quantum readiness**

PQC Essentials treats Post-Quantum Cryptography as an enterprise transformation rather than a purely technical upgrade. By completing structured discovery and migration planning upfront, organisations gain clarity, confidence, and a roadmap grounded in evidence, risk analysis, and operational reality. This ensures subsequent implementation activities are targeted, proportionate, and aligned to business, regulatory, and service continuity requirements.

## 1.4. Cryptographic dependency discovery

CGI can identify and assess cryptographic assets across IT and OT environments, including:

- Applications, platforms, and infrastructure.
- Data at rest, in transit, and in use.
- Third-party and supply-chain cryptographic dependencies.

Outputs include a cryptographic inventory, data life assessment, and prioritised risk heatmap highlighting services at greatest quantum risk.

# 2. Service Continuity

CGI works with clients to define quantum-safe continuity objectives, including:

- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for cryptographic services.
- Interim hybrid-cryptography approaches to maintain service availability.
- Controls to reduce disruption during algorithm transition.

This ensures critical services remain operational and trusted throughout PQC migration.

# 3. Onboarding and Offboarding

## 3.1. Onboarding

CGI engages with senior stakeholders to confirm scope, priorities, and regulatory drivers. Onboarding includes:

- Definition of business outcomes.
- Alignment to existing continuity and resilience frameworks.
- Secure mobilisation of cleared, PQC-specialist personnel.

## 3.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

### 3.2.1. Access to data upon exit

On service termination, CGI supports secure handover of artefacts, including cryptographic inventories, risk assessments, and continuity plans. All client data is securely handled and disposed of in line with contractual and regulatory requirements.

## 4. Service constraints

The service assumes:

- Availability of relevant architectural, security, and supplier documentation.
- Client sponsorship at senior leadership level.
- Timely access to technical and business stakeholders.

Specific constraints are agreed during service definition.

## 5. Service levels

The overall accountability for the relationship with the client lies with CGI's Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

## 6. Hosting options and locations

Services are delivered by UK-based CGI consultants, with on-site or remote delivery aligned to client security and operational requirements.

## 7. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organization to protect information assets, technologies, facilities and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organizational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these

additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

## 8. Service Pricing and Terms and Conditions

### 8.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

### 8.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

## 9. Further information

For more information about this or any of our G-Cloud services, please contact us:

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: [uk.gen.ccsframeworks@cgi.com](mailto:uk.gen.ccsframeworks@cgi.com), including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

## **PROPRIETARY AND CONFIDENTIAL**

The information contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765

