National Cyber Security Centre
a part of GCHQ

Assured Cyber Security Consultancy for the Post-Quantum Cryptography Pilot Offering

Standard

Version 1.0

May 2025

VERSION CONTROL				
Date	**Version**	**Change history details**	**POC**	**SharePoint Ref**
27/05/2025	1.0		Assured Cyber Security Consultancy Scheme Management Team	

A review will take place October – December of each year for publication the following February.

Document owner

National Cyber Security Centre (NCSC). All material is UK Crown Copyright ©

Abbreviations/Definitions

ACSC or the Scheme	Means the NCSC's Assured Cyber Security Consultancy Scheme.
ACSC Scheme Standard	Means the standards which must be met to be part of the ACSC Scheme. Referred to as the Standard.
ACSC Service(s)	Means cyber security consultancy service(s) offering independent consultancy to organisations with complex or high-risk cyber security requirements.
Agreement	Means the Ecosystem Agreement between the NCSC and the Company, including all Schedules, as amended from time to time.
Assured Service Provider Logo	Means the Assured Service Provider Logo as issued by the NCSC.
Company (and "Companies" shall be interpreted accordingly)	Means the company which is, or is applying to become, a member of the Scheme.
Customer	Means the organisation which contracts with the Company for ACSC Services.
Head Consultant (HC)	Means the person in the Company responsible for the technical aspects of ACSC Services.
NCSC	Means the National Cyber Security Centre.
NIST	Means the US National Institute of Standards and Technology.

Offering	Means a specific technical discipline assured under the Scheme.
Post-quantum Cryptography (PQC)	Means cryptography resistant to the threat from a future large-scale quantum computer. Primarily, this relates to asymmetric key establishment and signature mechanisms.
Service Owner (SO)	Means the person in the Company with overall responsibility for the provision of ACSC Services.
We/Us/Our	Means the NCSC.
Working Practices Document	Means the document setting out expected working practices in relation to the Scheme titled 'Assured Cyber Security Consultancy Scheme Working Practices'.
You/Your	Means the Company.

About the Assured Cyber Security Consultancy (ACSC) Scheme - Post-Quantum Cryptography (PQC) Pilot

Scheme Membership Requirements

1. The ACSC Scheme assures companies offering cyber security consultancy services to organisations with complex or high-risk cyber security requirements, across a range of consultancy Offerings.

2. This document defines the standards required for membership of the Assured Cyber Security Consultancy Scheme for the Post-Quantum Cryptography pilot only. It is split into two sections:

    - The Company Standard - Section A
    - The Offering Specific Standard – Section B

3. You must read this Scheme Standard in conjunction with the Working Practices Document and the Agreement. You must always (unless otherwise approved by the NCSC):

    - satisfy all the requirements defined in Section A of the Standard and the offering specific Annexe in Section B when providing the Offerings covered by such Annexe under the Assured Service Provider Logo.

    - meet the requirements of the overarching Ecosystem Agreement.

    - work in accordance with the Scheme Working Practices document.

    - be regularly delivering ACSC Services.

Section A – The Company Standard

Personnel

4. You must carry out all the activities identified in paragraphs 8 – 10 inclusive. We have divided them into two categories and assigned them to a role title. These role titles may not exist in your company, but we do expect there to be an identified person who is accountable to the NCSC for ensuring they are carried out.

    - Business requirements – “ACSC Service Owner”.

    - Technical Oversight and Health of the Company’s ACSC Service – “ACSC Head Consultant”.

ACSC Service Owner

5. While we do not expect one person to personally deliver all aspects of the ACSC service, the named Service Owner must be directly accountable for delivery of the service as a whole. Under the Scheme, the following tasks are all mandatory:

    a. Acting as the NCSC’s primary contact for all Scheme communications and all onward action.

    b. Positively contributing to the wider ACSC community. This includes:

        i. contributing to Scheme improvements.

        ii. taking an active part in community meetings.

        iii. meeting with the NCSC from time to time, as requested.

        iv. attend briefings from the NCSC on cyber security initiatives.

        v. contribute to consultations on NCSC initiatives.

vi. offer insights from your practice to influence NCSC initiatives.

c. Actively ensuring that the Company meets all its obligations under this Scheme and the associated Agreement.

d. Submitting, on time, an annual Management Information Report to the NCSC.

e. Documenting and maintaining Company Quality Management processes as they apply to the ACSC Service.

f. Reviewing and updating Company processes in accordance with the Scheme Standard.

g. Ensuring that everyone involved in the ACSC Service adheres to the Company's own documented processes.

h. Providing the Company's Cyber Essentials certificate number to the NCSC on an annual basis.

i. Actively monitoring and managing Customer relationships and seeking Customer feedback to provide evidence of Customer satisfaction with the Company's work.

6. The Company must have a business continuity plan that will aid in the continuity of ACSC Service(s) in the event of an accident, disaster or emergency, including staff unavailability.

7. The Company must be able to defend themselves against an appropriate level of cyber threat as defined in their own risk assessment, using good practice and their own specific or contracted-in skills.

ACSC Head Consultant

8. The named Head Consultant must be directly accountable for the technical quality of the ACSC Service, including the quality of the consultancy provided. The Head Consultant must be either a permanent employee or contractor and not employed or contracted for any ACSC-related work by any other company. The individual must have the capacity and capability to sign off all of the following mandatory tasks:

    a. Acting as the NCSC's primary contact for all technical and consultancy related questions and discussions and any onward action required.

    b. Ensuring that across the whole ACSC Service, and for every engagement, consultants use approaches and methods which are appropriate to the Customer and meet the highest, industry-accepted quality standards.

    c. Ensuring that every consultant delivers technical advice which is based on the most up-to-date thinking and practice. This includes ensuring that every consultant is familiar with the latest NCSC published advice and guidance and applies it during their engagements. Note that we do not expect the ACSC Head Consultant to personally lead and quality control every engagement, but we do expect the Company to have and adhere to a quality control process, for which the ACSC Head Consultant is accountable. This includes:

        i. ensuring the team members have an appropriate mix of expertise and experience to meet the Customer's needs.

        ii. conducting the engagement in accordance with the Company's methodology

        iii. ensuring the team's output meets the Company's quality standards.

        iv. accountability for the behaviours, actions and advice given by their team.

v. maintaining the overall competence of the consultancy team, both from a 'consulting' and 'technical' point of view.

d. You must ensure you and all of your consultants are, and remain, up to date with the public NCSC guidance and related technical advice presented on the NCSC website prior to delivering any ACSC Services. You must be able to apply this knowledge to the Customer's environment or be able to explain to the Customer why it is not appropriate.

e. You must be able to show how you keep all of your consultants up to date with actual and potential cyber threats and associated techniques, as well as effective mitigations. You must be able to apply your threat awareness to the Customer's environment.

Consultancy Lifecycle

9. You must have a documented and repeatable process for deciding the most appropriate consultancy approach for each engagement. The available approaches must be selected from the range of industry standard consultancy lifecycles and cover the entirety of an engagement from contracting to closure. Activities during the contracting phase must include, as a minimum:

    a. identifying the Customer's requirement, including exploring whether stated requirements achieve the intended outcome, and are appropriate and ethical for the level of risk the Customer is carrying;

    b. demonstrating that the Company has the capacity and capability to undertake the proposed package of work; and

    c. documenting and agreeing with the Customer the:

i. context of the work;

ii. services and deliverables, for example: risk assessment documentation, architectural plans, regular informal/formal updates, interim and final reports;

iii. approach and package of work;

iv. roles and responsibilities;

v. acceptance criteria; and

vi. terms and conditions.

10. During the “execution” phase, the Company must carry out the work agreed during the scoping phase using suitably qualified and experienced personnel. The Company must monitor their delivery and maintain regular contact with the Customer to ensure ongoing approval and acceptance of the outputs. In the event of any disagreement which cannot be resolved, the Company and Customer should document the issues and actions taken.

11. For the “closure” phase, activities should include:

a. final Customer evaluation and agreement that the work package(s) have been effectively delivered;
b. conclusion of contractual obligations;
c. feeding any lessons learned into the Assured Consultancy’s continual service improvement process; and
d. requesting and receiving Customer feedback.

Section B - The Consultancy Offering Specific Standard

Post-Quantum Cryptography (PQC) Pilot Offering

12. There are two separate but related Offerings for Post-Quantum Cryptography pilot, the requirements for which are below.

    - Post-Quantum Cryptography: Discovery and Migration Planning
    - Post-Quantum Cryptography: Advice

Post-Quantum Cryptography: Discovery and Migration Planning

13. This section defines the required technical capabilities to join the Consultancy Offering ‘Post-Quantum Cryptography pilot: Discovery and Migration Planning’.

Mandatory Defining Features

14. The purpose of the offering is to identify and prioritise data and services protected by cryptography that will be at risk from a future cryptographically-relevant quantum computer, to support Customers in planning for migration to post-quantum cryptography.

15. The requirements are deliberately intended to be flexible. That is, we recognise that PQC discovery and migration planning are large and complex activities, and that companies will make a range of contributions to the work, with some taking a more top-down, system-led approach, and others bringing deeper cryptography-led expertise. Each of these approaches can be recognised through the scheme.

Network Security

16. You must maintain an in-date Cyber Essentials certificate and be working towards Cyber Essentials Plus (CE+) certification for all the systems on which information relating to Customers' engagements is stored and processed.

Personnel

17. In addition to the personnel requirements set out in section A, you must meet the following requirements:

18. The Head Consultant must have sufficient personal expertise – from academic or commercial experience - to ensure that the Company maintains a strong core of knowledge of Post-Quantum Cryptography. This includes, but is not limited to:

    a. an appreciation of the characteristics, in both software and hardware, of the algorithms standardised through NIST's PQC standardisation project, and suitable use cases; and

    b. a strong understanding of the use of common cryptographic protocols, services and architecture in complex enterprises.

Technical Capability

19. The Company must demonstrate expertise in at least one of the following:

    a. Secure systems integration – identifying and managing critical components in Information Technology (IT) and Operational Techology (OT) systems, including key cryptographic components, and the data flows across them.
    b. Cryptographic security architecture – identifying the cryptographic services used to protect data in transit or at rest, and how they interact with wider systems within the client organisation and its supply chain.

c. Network discovery – application of tools or other techniques to identify configuration of cryptographic components.

20. The Company must ensure their outputs show awareness of developments in post-quantum cryptography, recognising that products implementing post-quantum solutions are still growing in maturity, and that protocols incorporating PQC are still undergoing standardisation.

21. You must produce well-defined outputs from your consultancy, explaining the implications of your analysis to Customers. These outputs must be clear and detailed enough to enable the Customer to make technical and business decisions to support their future migration to PQC. This must include:

a. assisting Customers with the assessment of risks to their data, based on its value and expected information lifetime;

b. identification of system or cryptographic components to enable Customers to define their early priorities for migration, either because they process higher risk data, or because migration is technically complex or involves components with slow refresh cycles;

c. suggesting additional discovery activities, including identifying supply chain dependencies; and

d. where you use proprietary tools as part of your analysis, you must present conclusions and assessment of risks clearly, in a way that supports decision-making by executives in Customer organisations.

Post-Quantum Cryptography: Advice

Mandatory Defining Features

22. This section defines the required technical capabilities to offer the Post-Quantum Cryptography pilot: Advice service.

23. You must be assured for the Offering Post-Quantum Cryptography: Discovery and Migration Planning to also be assured for Post-Quantum Cryptography: Advice.

Technical Capability

24. You must be able to show familiarity with the NCSC's published technical positions on Post-Quantum Cryptography and other cryptographic topics, and demonstrate that you can:

    a. Give advice that is consistent with those positions.
    b. Use that advice to contribute to Customers' future migration approach.
    c. Provide deeper consultancy on future cryptographic choices.

25. Where you have a UK Government and wider public sector Customer, this advice should precisely match the NCSC's guidance. We recognise that some clients operate in multiple regulatory environments, but advice must include components that are consistent with the UK's position.