National Cyber Security Centre
a part of GCHQ

# CORNERSTONE

## Market engagement prospectus

**First-phase opportunity for industry partners | November 2026**

# CORNERSTONE

## Purpose of this prospectus

> This document shares the NCSC's proposal for the first phase of Project CORNERSTONE and invites feedback from interested delivery partners. The first phase responds to urgent service needs and suggests capabilities that could form part of a wider future operating model.
>
> **Note: It does not define the full CORNERSTONE ambition and is not an invitation to tender.**

## At a glance

The NCSC is exploring how it can modernise the way its external services are designed, delivered and developed. We want to create an operating model that enables NCSC services to achieve greater impact, reach more organisations, respond more quickly to changing threats and technology, and make better use of the capabilities that exist across the cyber security market.

Our ambition is not simply to outsource services currently run by the NCSC. It is to develop a more scalable relationship between the NCSC and industry, with each focusing on where it can add most value. CORNERSTONE will make the NCSC's external services more impactful, accessible and adaptable, and will allow the NCSC to focus on those areas where it brings unique expertise as the national technical authority for cyber security.

This prospectus concerns the **first phase of CORNERSTONE**. It responds to immediate service needs, but it also gives us an opportunity to test some of the principles that could ultimately underpin a much broader operating model. The initial scope brings together **CHECK penetration testing, Assurance of Cyber Resilience Test Facilities (CRTF), and a new Protective DNS (PDNS) assurance service**, alongside common capabilities needed to support their operation. We are initially seeking market feedback on these three services.

This is early market engagement. We are **not inviting bids at this stage**, and the proposition set out here is not a settled commercial or delivery model. We want organisations with cyber security expertise and real-world experience of assurance and service delivery to help us test our thinking before any future competition.

CORNERSTONE's longer-term ambition is broader than the initial three services described in this prospectus. It is intended to explore a scalable operating model through which NCSC can govern, assure and enable a wider portfolio of external services, including both cyber assurance and Active Cyber Defence services, where industry delivery is appropriate.

# 1. CORNERSTONE's ambition

The NCSC's external services encompass both **Assured Industry services** and **Active Cyber Defence services.** They range from assurance schemes that help consumers identify providers meeting NCSC standards, to digital interventions that directly help organisations protect themselves from cyber threats. CORNERSTONE is intended to consider the future operating model across that broader portfolio, rather than simply improve individual services.

Our starting point is already a great success story: the NCSC's existing services have developed strong standards, trusted market relationships and significant reach. But as demand grows, it can be challenging to scale provision, introduce new services quickly, share capabilities between schemes, extract consistent data & insight, and focus scarce NCSC technical capacity on those activities that genuinely require specialist NCSC staff. These challenges extend beyond the three services in the first phase and inform the wider CORNERSTONE ambition.

CORNERSTONE is exploring whether a more coherent model can do better. Our longer-term ambition is a high-impact, collaborative and trusted marketplace in which organisations can confidently access NCSC-endorsed cyber security services. Industry has the space and incentives to invest, innovate and grow, and the NCSC retains the authority and expertise necessary to protect standards, outcomes and trust.

We are not assuming that every external service should eventually be delivered in the same way. Different services have different levels of maturity, technical sensitivity, market characteristics and dependencies. This is why this first phase is important. We want to move from operating-model theory to practical evidence. By bringing together a varied group of services, we can meet vital NCSC requirements, while also providing a foundation capable of accommodating further services over time.

**This first phase in CORNERSTONE therefore involves the market helping us to understand what is viable as we work towards a mature operating model**.

# 2. Proposed first phase

We are exploring a common delivery arrangement covering CHECK penetration testing, Cyber Resilience Test Facilities (CRTFs) and a new PDNS assurance scheme. Currently, CHECK and CRTF are distinct assurance schemes operated with significant NCSC involvement, while the existing PDNS contract is a different kind of service altogether. The proposed new PDNS assurance scheme would create something new rather than simply transfer the existing PDNS service into the arrangement.

The purpose of bringing these areas together is to explore whether there are **common administrative, data and operating capabilities** that can be provided more effectively across them.

These could include onboarding and managing assured organisations; running scheme administration and assurance processes; managing and processing data securely; providing common tools and infrastructure where appropriate; producing management information and insight; supporting the provider community; and continuously improving the way services operate. Our emerging work has consistently identified streamlined onboarding, high-quality assurance, shared infrastructure, stronger reporting and evidence, provider development and scalable joined-up delivery as common requirements.

Rather than prescribing a particular technology solution or detailed operating design, we are interested in what capabilities are required and how the market thinks they can best be delivered. Our proposed model is illustrative, and commercial terms have not been settled.

## Delivery models for the three schemes:

### 1. CHECK

CHECK is the NCSC's assured penetration testing scheme. It sets standards for penetration testing trusted by government, public sector and critical national infrastructure organisations. There are currently multiple assured CHECK providers, with customers contracting directly with them to conduct penetration tests. The NCSC currently retains total responsibility for the scheme, including its technical standard and scheme management.

**Under the proposed model**, we are investigating whether industry can take greater responsibility for scheme management, rather than the delivery of penetration tests. Customers would continue to contract directly with assured CHECK providers.

### 2. Cyber Resilience Test Facilities (CRTF)

The NCSC has developed a principles-based assurance methodology through which technology vendors can demonstrate the cyber resilience of connected products and services. Evaluations are undertaken by NCSC-assured Cyber Resilience Test Facilities (CRTF), while the NCSC provides the methodology, standards, branding and assurance framework.

**Under the proposed model**, we will explore how much of the assurance of those test facilities - confirming their capability to apply the NCSC's principles-based methodology - could be delivered through a common industry-led model. The focus is on assuring the facilities themselves, rather than transferring the NCSC's ownership of the methodology or its technical authority.

### 3. Protective DNS: an important distinction

**The existing NCSC PDNS service** is a live protective service. It prevents users from accessing domains or IP addresses known to contain malicious content by simply not resolving them and can prevent malware already within a network from communicating with malicious infrastructure. Its current delivery is contracted, and eligible organisations receive the protection through that service.

**The PDNS proposition within this first phase is a new NCSC assurance scheme, rather than an evolution or re-let of the existing service**. We are exploring the creation and operation of a new assurance scheme for providers of Protective DNS services. Rather than itself being the existing protective DNS service, the scheme would identify and assure providers that meet requirements approved by the NCSC, enabling organisations to select from trusted commercial services.

One attraction of including the new PDNS assurance scheme is that **it tests the feasibility of creating and scaling new schemes in partnership with industry.**

# 3. Proposed relationship between NCSC and industry

A central principle behind CORNERSTONE is that the NCSC should concentrate its expertise on activities where its position as the UK's national technical authority for cyber security is most beneficial. That does **not** mean simply transferring responsibility wholesale to an external organisation. We propose that the NCSC would remain the **root of trust**. We expect the NCSC to provide strategic direction, technical insight and knowledge of the threat landscape, and own and license use of the NCSC-assured brand. This includes responsibility for both:

- signing off new services
- ensuring that the authority behind standards and schemes is protected

We imagine a delivery partner (or potentially a group of organisations) taking greater responsibility for the **operating capabilities** surrounding those schemes. These could include:

- onboarding providers
- managing scheme administration and assurance processes
- providing secure data management
- management information analysis
- common tooling
- continuous improvement of services

We are also interested in a partner's ability to **help develop the marketplace** itself. A partner should not simply reduce NCSC administrative activities, and other activities might include:

- driving uptake of services
- surfacing better evidence of their impact
- proposing future developments for the NCSC's consideration
- enabling a delivery environment capable of adapting as technologies and threats evolve

The proposed future responsibilities for this first phase are summarised in the table below:

| NCSC's proposed retained responsibilities | Potential delivery partner responsibilities to test |
| --- | --- |
| • Brings technical insight and knowledge of the threat landscape.<br>• Owns scheme standards and protects the root of trust.<br>• Licenses use of the NCSC brand<br>• Approves new services as the national technical authority for cyber security. | • Onboards providers and manages scheme administration and assurance processes.<br>• Provides secure data management, MI analysis, common tools and continuous improvement.<br>• Implements approved services and proposes future development for the NCSC's consideration. |

# 4. Delivery partner expectations

This engagement will be most useful if potential partners understand the difference between **the outcomes and responsibilities the NCSC intends to retain** and **the assumptions that remain genuinely open to challenge**.

## Responsibilities retained by the NCSC

- The NCSC will remain the source of authority and trust behind its assured and digital services by owning the scheme standards.
- The NCSC will retain strategic oversight and technical authority, including approving new services.
- The NCSC will protect the integrity of its brand and determine the conditions under which it may be used.
- Appropriate independence and separation must protect the integrity of standards and assurance.
- The NCSC will require continued access to certain data to understand what is happening across industry, spot trends and improve its services.

## Our expectations of delivery partners

We currently believe that bringing the three schemes within a common delivery arrangement could generate economies of scale, reduce duplicated administration and create reusable capabilities. Potential delivery partner functions could include:

- managing provider onboarding and ongoing suitability processes for membership of NCSC assured services
- operating shared scheme administration and appropriate assurance processes
- managing and storing data in accordance with NCSC security requirements
- providing analysis, management information, impact evidence and practical recommendations for improvement
- supporting service agility so the marketplace can respond to technological and geopolitical change

Outcomes sought from the first phase delivery model can be summarised below:

| Ambition | What good could look like |
| --- | --- |
| **Streamlined onboarding and supplier management** | Consistent, efficient, rigorous and transparent end-to-end processes for providers joining, becoming assured and remaining suitable. |
| **Automation and shared infrastructure** | Less manual effort, duplication and unnecessary hand-offs, using common technology and capabilities where appropriate. |
| **Better data and evidence of value** | High-quality analysis, impact reporting and management information that supports service improvement and demonstrates performance and benefits. |
| **A stronger provider community** | Greater collaboration, awareness and responsible growth into new markets, sectors, and professional pathways. |
| **Scalable, joined-up delivery** | Reusable processes that support future services, align related schemes and enable more industry-led delivery where appropriate. |
| **Ways of working** | Optimal partnering behaviours such as open working, combined expertise, constructive challenge and joint resolution of issues. |

# 5. Who should engage?

This engagement is intended to improve our proposal before any procurement decision is made. We welcome responses from organisations with cyber security expertise and real-world experience of assurance, operating services at scale, scheme administration, integration, secure data or related capabilities.

## Why engage now?

| | |
|---|---|
| **Shape the first phase and inform the wider model**<br>Bring real-world delivery experience into the design of the immediate opportunity and help the NCSC understand which capabilities, governance arrangements and commercial approaches could be reused across the wider CORNERSTONE programme. | **Create opportunity**<br>Help explore a scalable market that can increase reach and create sustainable opportunities across the ecosystem. |
| **Collaborate and innovate**<br>Connect expertise, share knowledge and improve approaches for customers, providers and the wider market. | **Strengthen UK cyber resilience**<br>Help make trusted services more accessible and impactful for organisations across the UK economy. |

## Delivery and commercial assumptions to challenge

We are not expecting every organisation to have an answer to the following questions. We welcome challenge from prospective delivery partners, integrators, assurance bodies, cyber security providers, technology organisations and others who believe their experience can help us design a stronger approach.

**We welcome views on commercial and operational credibility.** The engagement is specifically testing whether CHECK, CRTF and the new PDNS assurance scheme form a sensible and coherent package and whether a lead delivery partner or integrator model is realistic. Are there material synergies between them, or important reasons why some elements should be treated differently?

**We welcome views on the role a delivery partner should perform.** Considerations here could include:

- Which responsibilities should sit with the NCSC, and which with delivery partners or assured providers?
- Could a single organisation realistically integrate the proposition while maintaining appropriate independence and quality?
- Should one organisation integrate the proposition, using specialist subcontractors or partnerships where necessary?
- Are there responsibilities that would be better divided differently to preserve trust?
- Which capabilities genuinely benefit from being common, and which need to remain scheme-specific?
- How can SMEs and specialist organisations participate without creating conflicts of interest or disproportionate barriers?

**We welcome views on our commercial assumptions.** We imagine a self-funding concession model. We therefore want evidence about where value is created, where costs and risks sit, what investment an operator would need to make, what revenue could reasonably support the model, and what contractual conditions would make participation sustainable and attractive.

Could the arrangement operate sustainably, and under what conditions?

Where would revenue be generated, what initial investment might be needed and what risk allocation would create an attractive but value-for-money proposition?

**We welcome challenge on deliverability, mobilisation and transition timescales**. We'd also welcome views on:

- the maturity of requirements, data and technology dependencies, the balance between prescription and operator freedom, and how continuous improvement should work
- where would shared onboarding, data management, tooling, reporting, assurance administration or other infrastructure create genuine value
- where would standardisation create unnecessary constraint

**We welcome views on market development and innovation.** How could the model increase participation and adoption, including opportunities for SMEs and specialist providers? How should the arrangement encourage continuous improvement rather than freezing today's services into a long-term contract?

# 6. What happens next?

This engagement is intended to inform our requirements, commercial thinking and approach ahead of any future competition. We anticipate a tender process beginning in **Spring 2027**, subject to the necessary governance and approvals.

Participation in this engagement does not create any commitment on either side. The NCSC has not committed through this exercise to undertake a procurement, award a contract or fund future activity. Any future opportunity will be subject to the relevant governance, approvals and procurement process.

What we want now is straightforward: **tell us what is viable, identify what we have missed, and help us make this first phase useful both in its own right and as a foundation for the wider CORNERSTONE ambition.**

Comments and questions can be sent to **cornerstone@ncsc.gov.uk**