



Government
Digital Service



Department for
Digital, Culture,
Media & Sport

Clarifications on the Cloud Challenge Book 2026

When we published the [Cloud Challenge Book](#) in July 2026, we invited industry to work with government to transform the UK's digital and AI capabilities through ambitious, innovative and scalable solutions.

Over summer 2026, GDS received written and verbal feedback on the Cloud Challenge Book from a range of suppliers. The questions below address common points raised through that engagement and clarify the outcomes government is seeking. In some areas, the engagement has also helped develop our thinking.

Challenge 1: Zero legacy public sector

What do we mean by legacy?

Government's [definition of legacy](#) is broader than ageing or unsupported technology. It can also include circumstances where public sector organisations lack the capability or capacity needed to maintain or improve a digital service. Upskilling our existing workforce can help address this but is not sufficient to address the challenge at the scale required.

How should we think about the role of different cloud services in addressing legacy?

Responses have identified how software as a service (SaaS) products, existing licensed products and cloud services can help government reduce legacy. These are all relevant to the wider challenge, which is deliberately focused on the outcomes government needs to achieve rather than a particular technology or service model. Where solutions rely on cloud infrastructure, our particular interest is in infrastructure as a service (IaaS), platform as a service (PaaS) and associated enabling services, which is the focus of future cloud infrastructure procurement.

Challenge 2: Public digital infrastructure for an AI era

What do we mean by resilient UK cloud regions?

For providers operating, or planning to operate, UK cloud regions, we want to understand their ability to support effective multi-region resilience within the UK. Our expectation is that this requires two UK regions with consistent access to the services, features and AI models that customers need to operate resilient workloads. Where material differences exist between UK regions, customers may otherwise need to design around unavailable functionality or accept reduced functionality if one region becomes unavailable. We would therefore welcome clarity on

current differences between UK regions and providers' plans and expected timescales for addressing them.

What infrastructure opportunities is government exploring?

Government is exploring whether public sector land and other assets could help support future cloud and AI infrastructure investment, particularly where access to suitable land and grid capacity may otherwise constrain development. For example, this could include a site which, subject to planning and investment, has the potential to support development at up to 40MW. We would welcome views from relevant providers on the characteristics they would require from potential sites, including the factors that would determine whether they are technically and commercially viable for investment.

Challenge 3: Secure-by-default, resilient-by-default cloud

This challenge is principally concerned with the security and resilience 'of' the cloud services government relies on, rather than how individual public sector organisations configure and operate their services 'in' the cloud. The latter remains important but is more closely related to the legacy and capability issues described under Challenge 1.

What do we mean by greater transparency and disclosure?

We expect transparency and disclosure to form an important part of future commercial arrangements for cloud services. Rather than developing requirements in isolation, we would welcome examples of the information, disclosures and assurances providers already make available to other national governments, where these can be shared, so that established approaches can inform the development of requirements for the UK government.

What does Cyber 4 mean by higher-security workloads?

While the Challenge Book is generally security-classification agnostic, Cyber 4 specifically relates to infrastructure capable of supporting workloads requiring what government would treat as SECRET-level protection. The Department for Digital, Culture, Media and Sport (DCMS) has formally acquired a mandate for SECRET Compute and AI infrastructure on behalf of government, Critical National Infrastructure (CNI), academia and industry, and intends to develop a demand forecast to better understand the scale and nature of that requirement. For clarity, activity relating specifically to TOP SECRET requirements is not within the scope of the Cloud Challenge Book.

Challenge 4: A cloud and AI expert nation

What role do we see for collaboration?

Feedback indicates interest from suppliers in collaborating on skills and capability, including approaches that bring together organisations across the cloud ecosystem and other sectors. We are interested in models that focus on measurable outcomes for government and create space for different organisations to contribute where they have relevant expertise.

What further feedback would be useful?

We would welcome views on the governance and delivery structures that would make collaboration effective, including how outcomes could be defined and measured, how

contributions from different organisations could be coordinated, and how a collaborative model could remain open to a broad range of participants.

Challenge 5: Commercial value at national scale

How does the Challenge Book relate to future commercial activity?

Where outcomes identified through the Challenge Book are best delivered through commercial arrangements, government expects future cloud infrastructure procurement activity to provide an important route for taking them forward. One anticipated procurement activity is the [National Cloud Infrastructure Programme \(NCIP\)](#) procurement, which is expected to launch in early 2027, subject to the programme's ongoing design and approvals.

What sort of commercial horizon is government considering?

Several of the outcomes in the Challenge Book, including investment in new UK infrastructure, will take a number of years to deliver. Responses to date have been based on a wide range of assumed timeframes. To support our understanding, we would ask suppliers to provide feedback on the basis of a horizon of five to ten years, and to set out how their response and the value they offer would differ across that range. This is a planning assumption for the purposes of engagement. The term, structure and nature of any future contractual commitments have not yet been decided and will be developed through the design of future commercial arrangements, with a continued focus on value for money, competition and flexibility.

We continue to welcome feedback from suppliers and other organisations able to contribute to one or more of the Cloud Challenge Book challenges through cloud-strategy@dsit.gov.uk.