

Application configuration and support within government-hosted cloud environments

1. Service definition

This service supports public sector organisations to configure, manage and support applications deployed within buyer-managed or government-hosted cloud environments. It focuses on application-level configuration, optimisation and ongoing support, working alongside internal hosting, platform and security teams.

The service does not include hosting, infrastructure provision or platform-level operations. It is delivered as professional cloud support services.

2. How the service works

The service is delivered through structured, time-bound engagements tailored to the buyer's needs. Activities may include application setup and configuration, alignment with platform constraints and policies, optimisation for performance and usability, application-level troubleshooting, and support for ongoing change and improvement.

Delivery is collaborative and works within the buyer's existing governance, security and hosting arrangements. Recommendations and actions are agreed with internal teams responsible for infrastructure and platform operations.

3. Onboarding and offboarding

Onboarding

Onboarding is delivered remotely and includes agreement of scope, objectives, success measures and ways of working. Buyers provide access to relevant applications,

documentation, environments and stakeholders. No infrastructure provisioning or platform configuration is performed as part of this service.

Offboarding

At the end of the engagement, configuration guidance, documentation, recommendations and any agreed outputs are handed over to the buyer. Knowledge transfer sessions can be included where required to support ongoing support and maintenance.

4. Service levels and support

Support is provided remotely via email and web-based support during UK business hours, Monday to Friday. Requests are acknowledged within one working day and prioritised based on urgency and impact.

Enhanced support, including extended availability or scheduled phone support, can be agreed at additional cost. As this is a professional services engagement, no infrastructure uptime or platform availability SLAs are provided.

5. Service constraints and customisation

The service is limited to application-level configuration and support within buyer-managed or government-hosted cloud environments. It does not include hosting, infrastructure management, platform operations or ownership of security controls.

The service is tailored through agreed scope and activities rather than bespoke software development or managed service provision.

6. Hosting and data

The service does not host buyer systems or operate cloud infrastructure. All infrastructure, platforms and environments remain under the control of the buyer or their appointed hosting provider.

Any working documents or analysis outputs are handled in accordance with agreed information governance and data protection requirements.

7. Security

The organisation follows documented information security policies covering access control, secure working practices, data protection and incident management. Responsibility for information security sits with a named board-level role.

Staff are subject to baseline security screening, with higher levels of clearance supported where contractually required and sponsored by the contracting authority.

8. Business continuity and resilience

As a professional services offering, resilience is supported through flexible resourcing, shared knowledge across delivery teams and contingency planning within engagements. Delivery is designed to minimise reliance on individual personnel.

9. Outage and maintenance management

The service does not operate hosted systems and therefore does not manage outages or maintenance windows. Any delivery disruption is managed through agreed delivery governance and communication with the buyer.

10. Data access and exit

All outputs created during delivery are provided to the buyer. No buyer data is retained beyond the end of the engagement unless explicitly agreed. Information is handled and disposed of in line with agreed data protection and retention requirements.