Security Services – Service Definition Document

G-Cloud 15: Lot 3 – Cloud Support

1. Service Overview

Our Cloud Security Services support public sector organisations in designing, operating, and assuring secure cloud environments. The service covers security strategy, risk management, secure cloud design, incident management, audit support, and security testing across public, private, and hybrid cloud platforms.

Our approach recognises that cloud security is an ongoing, operational activity rather than a one-off control implementation. Security risks are assessed continuously, reflecting the dynamic nature of modern cloud environments and distributed system architectures.

We support buyers in adopting security architectures based on continuous risk and trust assessment, enabling resilience while maintaining service availability. Our approach considers people, processes, and technology, ensuring that security controls are practical, proportionate, and aligned with organisational risk tolerances.

Security activities are designed to support business outcomes, protect information flows, and enable informed, risk-based decision making. We focus on clarity of accountability, ensuring that IT and security stakeholders can effectively fulfil their responsibilities.

Our services take a holistic view of cloud-based systems and services, providing coordinated security management that supports compliance requirements while enabling the buyer's organisational objectives.

Services are delivered by experienced cloud security professionals and are aligned with recognised good practice and UK government guidance.

The following services are included:

- **Security strategy** - We help buyers define or refine cloud security strategies, principles, and policies aligned with organisational objectives, regulatory requirements, and risk appetite. This includes guidance on security operating models, responsibilities, and governance structures.
- **Security risk management** - We identify, assess, and manage cloud security risks using structured risk assessment methods. Activities may include threat modelling, risk registers, and prioritised mitigation recommendations.
- **Security design** - We design and review secure cloud architectures, covering identity and access management, network security, data protection, encryption, logging, and monitoring. Designs focus on practical, proportionate controls suitable for cloud environments.
- **Security incident management** - We support the handling of cloud security incidents, including triage, investigation, coordination, and post-incident analysis. The service helps buyers improve response processes and reduce the impact of incidents.
- **Security audit services** - We provide security assessments and audit support, including control reviews, gap analysis, and evidence preparation against recognised standards and guidance.

- **Security quality assurance and testing** - We carry out security assurance activities such as configuration reviews, vulnerability assessments, and security testing of cloud environments and deployments.

This service offering is suitable for public sector organisations that:

- Are adopting or operating cloud services
- Need assurance over cloud security controls
- Require support responding to security incidents
- Want to improve their overall cloud security posture

2. Service Delivery

Our Cloud Security Services are delivered as a structured, risk-based engagement designed to help public sector organisations design, implement, operate, and continuously improve secure cloud environments. Services are delivered by experienced security professionals and aligned with recognised standards and best practices, including ISO/IEC 27001 principles and UK public sector security guidance, as well as Cyber Essentials Certificate.

The service begins with an initial engagement to understand the buyer's business context, regulatory requirements, existing cloud or hybrid environment, and risk appetite. Based on this understanding, we work collaboratively with stakeholders to define security objectives, scope, and priorities.

Services can be delivered remotely or on-site by experienced cloud professionals, according to buyer requirements, preferences and location. This is agreed before Call-Off Contract signing. Services can be delivered remotely or on-site by experienced cloud professionals, according to buyer requirements, preferences and location. This is agreed before Call-Off Contract signing.

3. Service Constraints

Delivery is dependent on timely access to relevant systems, documentation, and stakeholders. Scope is limited to the services agreed in the Call-Off Contract. Out-of-hours or emergency support must be agreed in advance.

4. Roles Involved

Services are delivered by experienced Cyber Security and Data Governance professionals. Buyers can view our complete role catalogue and fixed pricing directly on the Digital Marketplace service page.

5. Onboarding and Offboarding

Onboarding includes access setup, scope confirmation, and security briefing. The kick-off meeting will take place within 5 working days of Call-Off signature.

Offboarding includes knowledge transfer and handover of deliverables.

6. Certifications

- ISO 9001:2015 Quality Management System
- ISO 14001:2015 Environmental Management System
- ISO/IEC 20000-1:2018 IT Service Management system
- ISO/IEC 27001:2022 Information Security Management System
- Cyber Essentials Certificate of Assurance