



Service Definition

AI Security, Governance and Risk Management for Cloud Services

Supplier: Shivom Consultancy Limited

Framework: G-Cloud 15

Lot: Lot 3 – Cloud Support Services

Service overview

This service provides security, governance, risk management and assurance for cloud-based AI and machine learning services used by public sector organisations. It supports responsible, secure and compliant use of AI technologies across cloud environments.

Scope of the service

The service covers AI security risk assessment, governance framework design, assurance reviews, and compliance support for cloud-hosted AI and machine learning workloads. It applies to public cloud, private cloud and hybrid cloud environments.

Features

- AI security risk assessment for cloud services
- AI governance framework design and implementation
- Cloud AI threat modelling and risk analysis
- Security controls mapping for AI workloads
- AI model lifecycle security reviews
- Assurance for cloud AI service deployments
- Compliance assessment against AI regulations
- AI data security and privacy assessments
- Security architecture reviews for AI platforms
- Independent assurance reporting and recommendations

Benefits

- Improved security posture for cloud AI services
- Reduced AI-related operational and compliance risks
- Clear governance for responsible AI use
- Better assurance for senior stakeholders
- Stronger alignment with regulatory requirements
- Improved protection of sensitive AI data
- Reduced likelihood of AI security incidents
- Increased confidence in cloud AI deployments
- Clear accountability for AI risk management
- Independent validation of AI security controls

Service constraints

The service is delivered remotely unless otherwise agreed. It provides advisory, assessment and assurance support only and does not include managed security operations, continuous monitoring, or tooling procurement. Cloud licences, AI platforms and remediation implementation are excluded.

Onboarding and implementation

Onboarding includes an initial discovery session to confirm scope, objectives and stakeholders. Delivery activities are planned collaboratively and aligned to buyer governance and assurance processes.

Service management and support

Shivom Consultancy Limited provides flexible support levels tailored to buyer needs and the criticality of the service. Level 1 provides first-line support during UK business hours. Level 2 provides deeper technical support. Level 3 provides specialist expert-level support. Pricing is agreed at call-off.

Offboarding and exit management

At service completion, findings, reports and artefacts are handed over securely. Knowledge transfer sessions can be provided to support buyer continuity and internal capability development.

Security and data protection

All work is conducted in line with UK public sector security requirements. Data is handled securely, with access restricted to authorised personnel. No buyer data is retained beyond the engagement.

Accessibility

Where documentation or support portals are provided, accessibility is considered in line with WCAG 2.2 AA standards, including compatibility with assistive technologies.

Pricing

Pricing is agreed at call-off and depends on scope, duration and depth of financial and sustainability analysis required. All pricing is transparent and documented in the call-off contract.