Service Definition

AWS Cloud Security Assurance, Audit and Incident Support

Supplier: A&A Digital Tech Ltd
Framework: G-Cloud 15
Lot: Lot 3 – Cloud Support Services

1. Service overview

A&A Digital Tech AWS Cloud Security Assurance, Audit and Incident Support services provide specialist security assurance, audit and incident response support for workloads hosted on Amazon Web Services (AWS). The service helps organisations maintain a strong security posture, meet assurance requirements and respond effectively to security incidents in live cloud environments.

2. Scope of the service

The service covers security assurance reviews, audit support and incident response activities for AWS-hosted environments. It supports compliance, risk management and operational security activities. The service does not include continuous managed security operations or tooling provision unless explicitly agreed at call-off.

3. Features

AWS security architecture and configuration assurance reviews
Security risk assessments and threat modelling
Support for security audits and compliance evidence
Review of AWS security controls and guardrails
Identity, access and privilege configuration reviews
Security logging and monitoring configuration review
Security incident triage and response support
Forensic support and incident investigation assistance
Post-incident analysis and remediation recommendations
Security assurance reporting and documentation

4. Benefits

Improved security posture of AWS environments
Reduced risk of security misconfiguration
Clear evidence for audits and assurance reviews
Faster and more effective response to security incidents
Improved visibility of security risks and controls
Better alignment with AWS and public sector security best practices
Reduced impact and duration of security incidents
Improved confidence in cloud security arrangements
Clear remediation actions and improvement plans
Support for secure and compliant cloud operations

5. Service constraints

The service can be delivered remotely, on-site, or using a hybrid delivery model, depending on buyer requirements and agreement at call-off. Effective delivery depends

on timely access to AWS environments, security logs, documentation and authorised personnel provided by the buyer. The service provides advisory, assurance and incident support activities only and does not replace buyer responsibilities for security ownership or statutory reporting unless explicitly agreed.

6. Onboarding and implementation

Onboarding includes confirmation of scope, security objectives, environments and escalation procedures. Activities are delivered in structured phases aligned to assurance, audit or incident response requirements.

7. Service management and support

Support is provided in line with agreed support levels. A named security specialist can be provided to coordinate assurance activities, manage incidents and act as a single point of contact during security events.

8. Offboarding and exit management

At the end of the engagement, A&A Digital Tech provides agreed assurance reports, audit evidence and incident documentation. No buyer data is retained beyond the end of the contract unless otherwise agreed.

9. Security and data protection

A&A Digital Tech follows UK government cloud security principles and NCSC guidance. Staff screening is performed in line with BS7858:2019. Buyer data accessed during security activities is handled in accordance with UK GDPR and contractual data protection requirements.

10. Accessibility

This document is written in plain English and structured using accessible headings. Security reports and documentation can be provided in accessible formats where required.

11. Pricing

Pricing is agreed at call-off and depends on scope, environment complexity, assurance depth and incident response requirements. All pricing is transparent and documented in the call-off contract.