Service Definition

Microsoft Azure Security Assurance, Audit and Incident Support

Supplier: Shivom Consultancy Limited
Framework: G-Cloud 15
Lot: Lot 3 – Cloud Support Services

shivom

Service overview

This service provides security quality assurance, security audit support, and security incident management for Microsoft Azure environments. It supports public sector organisations in validating Azure security controls, reviewing configurations, and managing security incidents using Azure-native services.

Scope of the service

The service covers Azure security posture reviews, security QA testing, audit preparation support, and incident response assistance. It applies to Microsoft Azure subscriptions and Azure-native services including identity, networking, logging, monitoring, and security management services.

Features

Azure security posture reviews
Security QA testing against Azure controls
Azure configuration and policy assessment
Security audit evidence collection support
Azure logging and monitoring review
Incident response coordination support
Azure security incident investigation
Root cause analysis for incidents
Security control validation testing
Remediation recommendation reporting

Benefits

Improved Azure security assurance
Reduced security misconfiguration risk
Stronger audit readiness
Faster incident response handling
Clearer security control visibility
Improved compliance confidence
Reduced operational security risk
Improved incident investigation outcomes
Better-informed security decisions
Enhanced cloud security governance

Service constraints

Services are delivered remotely during UK business hours unless agreed otherwise. Buyers must provide appropriate Azure access, documentation, and stakeholder availability. This service excludes penetration testing, managed SOC services, security tooling provision, and cloud consumption costs.

Onboarding and implementation

Onboarding includes confirmation of scope, access setup, and engagement planning. Delivery is coordinated with buyer stakeholders and aligned to agreed security objectives, timelines, and reporting requirements.

Service management and support

Shivom Consultancy Limited provides flexible support levels tailored to buyer needs and the criticality of the service. Level 1 support provides first-line support for service queries, incident logging, basic troubleshooting and request handling during UK business hours. Level 2 support provides second-line technical support, including deeper investigation, issue resolution and configuration support, with extended hours available by agreement. Level 3 support provides specialist and expert-level support, including complex fault resolution, architectural input and escalation handling. Support costs vary depending on the selected support level, hours of coverage and service scope. Pricing is agreed with the buyer at the start of the engagement and detailed in the call-off contract. A named technical account manager or cloud support engineer can be provided for Level 2 and Level 3 support.

Offboarding and exit management

Offboarding includes knowledge transfer, handover of documentation, and confirmation of access removal. Exit activities are agreed with the buyer to support continuity and security.

Security and data protection

The service follows UK public sector security principles and supports buyer security policies. Access is limited to agreed Azure resources. No buyer data is retained beyond the engagement without written agreement.

Accessibility

Where documentation or support portals are used, accessibility considerations are reviewed periodically. This service aligns with WCAG 2.2 AA accessibility standards.

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.