Service Definition

Cloud Support Services – Security Services

We provide end-to-end cloud security support for public sector organisations adopting and operating cloud services. Our specialists help you define security strategy, manage risk, design and review secure cloud architectures, assure delivery quality, prepare for and respond to security incidents, and demonstrate compliance through audit and assurance activities. The service is designed to strengthen security governance and controls across the full cloud lifecycle, from initial strategy and design through to live service operations and continuous improvement.

Service scope and outcomes

This service covers the following security capabilities across public sector cloud environments:

- Development of cloud security strategy, policies, guardrails, and governance aligned to public sector standards and organisational risk appetite.
- Contextual cloud risk assessments, threat modelling, and definition of proportionate controls and mitigations.
- Secure architecture patterns, control designs, and design reviews for new or changed services, including identity and access management (IAM) and data protection.
- Proportionate security testing and independent assurance of buyer/supplier testing.
- Incident response planning, playbooks, exercises, and readiness reviews to improve time to detect and time to respond.
- Independent audit and assurance activities, evidence preparation, and support for accreditation and external reviews.
- Security assurance embedded across delivery lifecycles, from design and build through to pre-production verification and go live readiness.

Expected outcomes include:

- A clearly articulated cloud security strategy and governance model that clarifies shared responsibility and supplier assurance expectations.
- Reduced security and compliance risk through proportionate controls, secure design decisions, and remediation plans.
- Assured designs and configurations via structured reviews of architectures, configurations, and IAM.
- Improved incident readiness and response through actionable playbooks and scenario based preparations.
- Demonstrable compliance with relevant standards via audit ready evidence, findings, and assurance reports.

- Continuous improvement of cloud security posture through prioritised remediation and measurable follow up actions.

Engagement planning and design

We plan each engagement to reflect your organisational context, cloud platforms, regulatory obligations, and delivery cadence. Typical preparation includes:

- Understanding scope, stakeholders, critical assets, architectural landscape, and threat profile.
- Agreeing the applicable standards, policies, and frameworks to align with (e.g., UK public sector guidance, internal governance, and assurance needs).
- Selecting appropriate methods and depth for risk assessment, threat modelling, architecture review, configuration assessment, and QA/assurance activities.
- Defining success criteria, artefacts, and evidence requirements to support audit, accreditation, or gateway/assurance checkpoints.

Security design, review, and assurance activities

We deliver expert led advisory and review activities that strengthen cloud security by design and by operation:

- Secure architecture and design reviews of services, integrations, and data flows, including control coverage and defence in depth considerations.
- Cloud risk assessment and threat modelling to identify threats, attack paths, and control gaps, with pragmatic mitigation options.
- Identity and access management (IAM) design and assurance, including role design, privileged access, conditional access, and federation patterns.
- Configuration reviews of cloud platforms and services against recognised security baselines and best practice; identification of misconfigurations and improvement opportunities.
- Incident response planning and playbooks for priority scenarios; table top exercises to validate roles, processes, and decision paths.
- Security QA across delivery lifecycles, assuring non functional security requirements, test evidence, and go live readiness.

Security QA and Testing

We provide proportionate security testing services or coordination/oversight of buyer/supplier testing, including vulnerability assessments, penetration testing scoping and supplier management, security test planning & evidence review, build/configuration hardening checks, and security test automation advisory. Where direct execution is out of scope, we offer independent assurance of third-party testing and acceptance criteria.

Security Incident Management

Advisory across the end-to-end incident management lifecycle, including preparedness, detection/triage process design, escalation paths, communications, recovery planning, post-incident reviews, and continuous improvement. We develop or review RACI, runbooks, and metrics (e.g., MTTD/MTTR).

Security Audit Services

Audit planning, readiness assessments, evidence mapping, and audit execution support against agreed frameworks; independent findings, risk statements, and management action tracking; support for gateways/accreditation.

Security Design

Control design, reference patterns, and design decisions/waivers covering identity, data protection, network segmentation, key management, and zero-trust guardrails, with defence-in-depth

Security Strategy

Cloud security strategy and governance model, shared responsibility, supplier assurance expectations, and guardrails.

Security Risk Management

Ongoing risk identification, assessment, treatment planning, and residual-risk tracking aligned to enterprise risk, with threat modelling and risk-based prioritisation.

Findings, assurance outputs, and recommendations

On completion of scoped activities we provide clear, evidence based outputs:

- Findings and risk statements with business impact, likelihood, and prioritisation.
- Assurance conclusions that explain the strength of controls and residual risks.
- Practical remediation guidance with target states, quick wins, and roadmap proposals.
- Audit and compliance evidence packs aligned to agreed frameworks or checkpoints.
- Executive summaries that support governance decisions and investment prioritisation.

Deliverables

Depending on scope, deliverables may include:

- Cloud security strategy documents, guardrails, and governance playbooks.
- Risk assessments and threat models for services, platforms, or changes.

- Secure architecture review reports and design decisions/waivers.
- IAM design guidance, patterns, and assurance statements.
- Incident response plans, role matrices, and scenario playbooks.
- Audit and assurance reports, evidence checklists, and accreditation support materials.
- Security improvement plans and prioritised remediation backlogs with acceptance criteria.

Service delivery approach:

Discovery and security assessment

We begin by understanding your cloud landscape, business objectives, regulatory drivers, and existing controls. We confirm scope, stakeholders, artefacts to review, and desired outcomes, and agree a statement of work covering delivery methods and cadence.

Security design and assurance planning

We tailor the approach for risk assessment, threat modelling, architecture and configuration reviews, IAM analysis, incident readiness, and QA/assurance. We define artefacts, checkpoints, and success measures.

Security advisory delivery and support

We execute the agreed activities, engaging with architects, delivery teams, service owners, and suppliers. Advisory sessions, reviews, and walkthroughs are used to validate decisions and collect evidence.

Security assurance, incident readiness, and improvement planning

We synthesise findings into actionable recommendations, confirm remediation priorities, and (if required) rehearse incident response scenarios and go live readiness.

Knowledge transfer and governance handover

We provide the agreed documentation, evidence, and guidance to support internal governance, ongoing risk management, and supplier assurance.

Engaging with us

Once you have conducted your search on the digital marketplace and followed the appropriate process to identify us as a possible supplier, beginning your journey with us is simple. It starts with a conversation with one of our Partners to ensure that we

can deliver to your needs; if we have any reservations about our ability to deliver then we commit to provide honest feedback without charge.

If both parties feel that we can establish a constructive working relationship, then we will move to support you as necessary with the completion of the G-cloud order form. We will complete any required paperwork in the timeliest manner possible to ensure that a call-off contract can be raised rapidly, along with the relevant terms and conditions. Invoicing is in arrears aligned to the statement of work and or time & materials delivered.

Onboarding

Service onboarding will commence within a few days of the completion of paperwork. We confirm objectives, scope, artefact lists, stakeholder availability, delivery schedules, and reporting arrangements to ensure a smooth start and timely access to required information and environments.

Implementation

This service provides advisory, assurance, and specialist cloud security expertise. It does not include the implementation, configuration, or operation of cloud platforms, security tools, or service desk functions unless separately contracted and explicitly scoped

Performance reporting

We agree service levels and reporting frequency at the outset and reflect these in the statement of work. You will have direct access to a Partner for oversight and escalation. We recommend weekly reporting in month one, moving to fortnightly in month two and monthly thereafter. Reporting highlights objectives, activities completed, findings emerging, risk changes, and remediation progress.

Milestone confirmation and efficiency analysis

At the half-way point of the project or following the third month, we will invite you to undertake a review meeting with the Managing Partner. At this point and via an open and honest dialogue, we will reconfirm the delivery objectives within the statement of works with the intention of reducing timelines and costs. This crucial engagement also provides an excellent opportunity to highlight any areas of outstanding performance or concerns and to reconfigure service delivery if required.

Service constraints

Our service provides advisory, assurance, and specialist cloud security expertise. We do not provide cloud infrastructure, hosting, or service desk operations. Services are delivered by experienced security professionals and specialist practitioners selected to meet buyer requirements. Ongoing operational activities, tooling, and run time responsibilities remain the buyer's responsibility unless explicitly agreed within a defined engagement scope.

Data Hosting & Processing

This service does not include hosting, storing, processing, or managing customer production data or cloud environments. All work is advisory or security-assurance focused. Any artefacts produced relate only to security strategy, risk assessment, secure architecture, assurance activities, or related security guidance.

Security and assurance

This service operates at OFFICIAL and does not process, store, or persist any customer production data. All work is advisory or security-assurance focused and is delivered by experienced cloud and security professionals, including personnel with appropriate security clearances for sensitive environments (e.g., defence/justice) where required and agreed. All activities are performed strictly within the scope, governance, and security controls defined by the buyer to maintain the confidentiality, integrity, and availability of their information and systems.

Backup, Restore, Business Continuity & Disaster Recovery

This service does not relate to any Buyer IT systems, environments, workloads, or production data. We do not host, operate, or manage any Buyer systems or security tooling. Backup and business continuity measures apply only to:

- supplier-managed project artefacts stored within our secure collaboration tools
- continuity of consultancy and security-assurance service delivery

No infrastructure, security platform, or production workload disaster recovery is provided or required for this advisory and assurance service.

Offboarding

At completion we provide the agreed artefacts, evidence, and recommendations, confirm delivery of outputs, and hand over materials necessary for continued governance, remediation tracking, and internal assurance.

Access to Artefacts on Exit

All deliverables and artefacts created during the engagement will be provided to the Buyer in open, accessible formats. As the service does not host or store customer production data, no data extraction or migration services apply

Termination

Our standard termination period is 10 working days, however, subject to agreement and the operational practicalities of termination, we may accommodate shorter periods of notice where possible.

Customer contributions

We request the following of our clients:

- Prompt confirmation or approval of any deliverables, expenses or time and materials related documentation if applicable;
- Access to the required technology, systems, documentation, and team members to allow deliverables to be achieved;
- Holding or sponsoring any security clearances as may be required;
- Sufficient provision of time and/or data to allow deliverables to be completed.

Technical Prerequisites

To deliver the service effectively, the Buyer must provide access to relevant architectural artefacts, security policies, governance documentation, and appropriate stakeholders. No access to technical infrastructure, cloud environments, security tooling, hosting platforms, or elevated permissions is required, as all work is advisory and security-assurance focused.