

Service Definition – Security Services

1. Service Overview

Guidehouse's Security Services help public sector organisations strengthen their cloud security posture through structured assessment, design, assurance and incident response capabilities. The service covers risk assessment, secure architecture, security controls implementation, audit and compliance, incident planning and testing. It aligns closely with NCSC cloud security principles and ISO 27001, providing clear, plain-English guidance suitable for buyers without deep security expertise.

This service is suitable for organisations seeking to reduce security risk, achieve compliance, and build confidence in cloud environments.

2. Service Scope & Objectives

Scope

The service includes:

- Security strategy and roadmap development
- Security risk assessment, threat modelling and mitigation definition
- Secure architecture design and patterns for cloud workloads
- Security controls design (IAM, encryption, logging, governance)
- Incident response planning, playbooks and response support
- Security audits and compliance assessments (including gap analysis)
- Security QA/testing, such as configuration reviews and penetration testing

Objectives

- Strengthen cloud security maturity and governance
- Reduce risk via structured, evidence-led assessments
- Improve compliance with public sector security standards
- Enhance detection, response and resilience capabilities
- Provide buyers with confidence in cloud operations and architecture

3. Service Features & Benefits

Features (from Lot 3 Consolidated Responses)

- Security strategy and roadmap
- Security risk assessment, threat modelling and mitigation
- Secure architecture patterns for cloud workloads
- Security controls design (IAM, encryption, logging, governance)
- Incident response planning and execution
- Security audits, compliance assessments and gap analysis
- Security QA/testing including penetration testing and configuration reviews

Benefits

- Improved cloud security maturity and governance
- Reduced organisational risk via structured assessments and testing
- Clear alignment to NCSC principles and public-sector standards
- Stronger detection, response and resilience
- Increased assurance and confidence in cloud operations

4. Service Components / Work Packages

4.1 Assess & Prioritise

- Security risk assessments, threat modelling and control gap identification
- Compliance baselining against NCSC and ISO 27001
- Prioritised remediation roadmap

4.2 Design & Enable

- Secure architecture patterns and reference designs

- Identity, access, encryption and logging controls
- Governance frameworks and policy design

4.3 Validate & Assure

- Configuration reviews and build assessments
- Penetration testing and vulnerability analysis
- Evidence-based assurance reports and remediation guidance

4.4 Respond & Improve

- Development of incident response processes and playbooks
- Table-top simulations and response exercises
- Post-incident reviews and improvement recommendations

5. Roles & Responsibilities

Guidehouse Responsibilities

- Provide security architects, analysts and testers
- Deliver all assessments, designs and testing outputs
- Coordinate with Buyer teams and third parties
- Ensure staff are vetted to **BS7858:2019** and **SC-level** where needed

Buyer Responsibilities

- Provide access to relevant systems, logs and personnel
- Approve remediation activities and control implementations
- Provide availability for interviews, workshops and testing windows

6. Onboarding & Offboarding

Onboarding

- Scoping workshop and objectives validation
- Access and documentation review
- Confirm testing windows and assessment criteria

Offboarding

- Handover of deliverables and reports
- Knowledge transfer sessions
- End-of-engagement recommendations and roadmap review

7. Service Management & Reporting

- Regular reporting on risk levels, compliance posture and remediation progress
- RAID management where required
- Incident exercise and test reports
- Support accessible via email, phone, ticketing and **WCAG 2.2 AA-compliant** web chat during UK business hours

8. Security, Compliance & Standards

- Aligns to NCSC cloud security principles and ISO 27001
- Staff vetted to BS7858:2019 and up to SC clearance
- Data protection and confidentiality handled in accordance with **CCS General Terms**, with no modifications

9. Constraints & Dependencies

Dependencies

- Access to logs, configurations and systems
- Availability of Buyer SMEs
- Agreed maintenance or testing windows

Constraints

- No intrinsic constraints declared in Guidehouse's tender submission

- This Service Definition does not modify or replace CCS General Terms

10. Pricing Model (Non-Commercial Description)

Pricing is based on published Lot 3-day rates. Work is typically delivered as time-and-materials, with optional fixed-scope assessments or testing packages available. Pricing excludes VAT and travel/subsistence and complies with CCS pricing rules.

11. Document Control

- **Service Name:** Security Services
- **Supplier:** Guidehouse
- **Framework:** G-Cloud 15 – Lot 3 Cloud Support
- **Related documents:**
 - CCS General Terms (RM1557.15-v1.0)
 - Lot 3 Consolidated Service Responses
 - RM1557.15 Attachment 2 – How to Tender
 - Guidehouse Overarching Lot 3 T&Cs

This Service Definition must be read alongside the above documents and does not override CCS General Terms.