SERVICE DEFINITION DOCUMENT

Service Name: NCSC-Aligned Cloud Security Architecture, Risk & Assurance Service

Provider: Secure Equinox Limited

G-Cloud 15

Reference: Jan 2026

---

1. Service Overview

Secure Equinox Limited delivers NCSC-aligned Cloud Security Architecture and Information Assurance led by SC/DV-cleared Principal Architects with 20+ years' experience securing regulated environments (Financial Services, Defence, Healthcare, Public Sector).

We accelerate secure cloud adoption for UK Public Sector organisations—Central Government, NHS, Defence, and Law Enforcement—ensuring compliance with NCSC Cloud Security Principles, HMG Security Policy Framework, and Zero Trust Architecture requirements. Our expertise spans AWS, Azure, and Microsoft 365 security architecture.

We bridge the gap between complex technical implementation and formal security governance, accelerating your path to Authority to Operate (ATO) while building internal team capability through knowledge transfer.

2. Key Service Features

- NCSC-aligned Cloud Security Architecture and Design (AWS/Azure).
- Security Risk Management and Assurance (ISO27001, NIST, GDPR).
- SC and DV Cleared Principal Consultants (20+ years' experience).
- IT Health Check (ITHC) and Penetration Testing Management.
- Strategic Security Leadership and Virtual CISO Services.
- Secure Cloud Migration Strategy and "Secure by Design" adoption.
- Supplier Assurance and Third-Party Risk Management (TPRM).
- HMG Accreditation Support and GDS Service Standard compliance.
- Zero Trust Architecture (ZTA) design assurance aligned with NCSC principles.
- Cyber Essentials and Cyber Essentials Plus readiness assessment and certification support

3. Key Service Benefits

- **Rapid Accreditation:** We accelerate the path to "Authority to Operate" (ATO) by ensuring designs are compliant from day one.
- **High-Grade Expertise:** Direct access to SC/DV cleared experts with deep experience in high-threat environments.
- **Cost Efficiency:** We provide senior-level guidance without the overheads of large generalist consultancies.
- **Knowledge Transfer:** We mentor internal civil service teams to build long-term in-house capability.
- **Vendor Independence:** Our advice is technology-agnostic and focused solely on your risk appetite.
- **Proven regulated environment expertise:** Financial Services (FCA/PRA), Healthcare, Defence, Critical National Infrastructure.
- **Flexible engagement models:** Remote, on-site, or hybrid delivery to suit your needs.
- **Vendor-independent advice:** Technology-agnostic recommendations focused on your risk appetite.

4. Key Deliverables

Architecture & Design Documentation:

- High-Level Design (HLD) and Low-Level Design (LLD) documents aligned to NCSC Cloud Security Principles.
- Network Architecture Diagrams (logical and physical topology).
- Data Flow Diagrams showing information classification and boundary controls.
- Zero Trust Architecture design assurance with identity, device, network, and application controls.

Risk & Assurance Documentation:

- Risk Register with quantified likelihood/impact scores aligned to departmental risk appetite.
- Risk Treatment Plan with prioritized remediation roadmap.
- Business Impact Assessment (BIA) for critical services and data assets.
- Threat Model using STRIDE or similar methodology identifying attack vectors.
- Security Risk Management Document supporting HMG accreditation processes.
- Statement of Compliance mapping implemented controls to ISO 27001, NIST CSF, or Cyber Essentials.

Governance & Compliance:

- Security Operating Procedures (SyOPs) defining user responsibilities and secure usage.
- Statement of Compliance mapping controls to ISO 27001, NIST CSF, or Cyber Essentials.
- Shared Responsibility Matrix (RACI) for cloud security between provider and customer.
- Authority to Operate (ATO) supporting documentation.

Testing & Validation:

- IT Health Check (ITHC) Scoping Document defining test boundaries, rules of engagement, and success criteria.
- ITHC remediation tracker with risk ratings and closure evidence.
- Vulnerability Assessment scope and remediation plan.

Supplier & Third-Party Assurance:

- Third-Party Risk Assessment for cloud providers (AWS, Azure, GCP)
- Supplier Security Questionnaires and due diligence reports
- Cloud Service Provider assurance mapping to NCSC 14 Principles
- Supply Chain Risk Management (SCRM) documentation

Operational Documentation:

- Security Monitoring and Logging Framework (what, where, how long)
- Incident Response Plan with escalation procedures and contact details
- Backup and Disaster Recovery Plan with RTO/RPO definitions
- Access Control Policy with identity lifecycle and privilege management
- Patch Management Policy and schedule

Knowledge Transfer:

- As-Built Documentation handover with system walkthrough
- Security Hardening Guides for administrators
- Operational Runbooks for routine security tasks

Note: Deliverable selection is tailored to engagement scope and objectives. Not all deliverables are required for every engagement. During onboarding, we agree a specific deliverable list matching your accreditation requirements, organizational standards, and budget constraints.

5. Our Approach & Methodology

We utilize industry-standard frameworks tailored to the specific classification of your data:

- **Architecture:** We produce High-Level Designs (HLD), Low-Level Designs (LLD), and Zero Trust Architecture blueprints aligned with NCSC Cloud Security Principles and industry best practice.
- **Risk:** We deliver Risk Registers, Threat Models, and Risk Treatment Plans using ISO 31000/27005 and NCSC Risk Management guidance.

- **Assurance:** We provide independent security validation through architecture reviews, ITHC management, compliance audits, configuration assessments, and control testing. We produce Security Cases, Statements of Compliance, Remediation Trackers, and complete evidence packages to support Authority to Operate (ATO) decisions.

6. Onboarding and Offboarding

- **Onboarding:** Engagement typically begins with a 1-day scoping workshop to define the boundary, stakeholders, and key deliverables. We can mobilize resources within 5–10 working days.
- **Offboarding:** All engagements conclude with a formal handover of documentation (High-Level Designs, Risk Registers, SyOPs) and a skills transfer session to permanent staff. All data is securely deleted or returned in line with GDPR.

7. Service Constraints

- Consultants are UK-based.
- On-site working is available by arrangement (standard travel expenses apply).
- Minimum engagement duration is typically 5 days.

8. Pricing

Pricing is based on our G-Cloud SFIA Rate Card.

- **Standard Rate:** Our published rates apply across all relevant SFIA categories (Strategy & Architecture, Business Change, Solution Implementation, etc.), reflecting the cross-functional nature of Security Architecture and Assurance. Fixed-price quotations available for defined scopes. Flexible engagement models (time & materials, fixed-price project, or retained advisory) to suit varying procurement needs.
- **Discounts:** Educational or volume discounts are not generally applicable due to the specialist nature of our resources. However, preferential rates for significant, strategic engagements (e.g., multi-year programmes) may be discussed at the Call-Off stage.

9. Technical Requirements

We do not require specific software installation. We can operate using our own secure IT or client-issued devices where higher classification processing is required.

[End of Document]