Cyber Security and Information Assurance

Service Definition Document

G-CLOUD 15

EVODIA LIMITED
8 St. George's Yard, Castle Street, Farnham, Surrey GU9 7LW
info@evodia.co.uk | 01252 722500 | www.evodia.co.uk

FS 55799

Contact Us

If you have a Framework related question or query, please find our contact details below.

Our contact details: +0044 (0)1252 722500

info@evodia.co.uk

Service Definition – Cyber Security and Information Assurance

1. Overview

We help public-sector organisations design, assure and evidence secure digital and cloud services. Our focus is on cloud security architecture, information assurance (IA) strategy, policy development, risk assessments, secure-by-design guidance, penetration testing, and digital forensics—all aligned to UK government standards and best practice. We enable programmes to reduce risk, protect sensitive data, and deliver compliant outcomes at pace.

What this service is for:

- Supporting discovery-to-live delivery of digital public services
- Assuring cloud migrations and modernisation programmes
- Demonstrating compliance and readiness for governance gateways and audits
- Identifying and remediating vulnerabilities before they affect citizen services

2. Scope of Service

Core Capabilities

Cloud Security Architecture

- Reference architectures, landing zones, guardrails and control patterns
- Secure configuration baselines for AWS, Azure, M365 and hybrid environments
- Identity, access, network segmentation, encryption, key management, logging design

Information Assurance Strategy

- IA operating model, roles, RACI and governance cadence
- Risk appetite statements, assurance plans, service accreditation support
- Alignment to NCSC guidance, NIST CSF, Government Functional Standard GPG and ISO 27001

Policy Development & Governance

- Security policy suite drafting, updates and harmonisation
- Standards, secure coding guidelines, exception management
- Board and senior-stakeholder briefings, decision papers and governance templates

Risk Assessments

- Threat modelling, risk identification, scoring and treatment planning
- Cloud control effectiveness reviews against recognised frameworks
- Supplier and third-party risk assessments (incl. data processors)

Secure-by-Design Guidance

- Security requirements for procurement and delivery teams
- Design reviews, architecture decision records, pattern approvals
- Shift-left security guidance for agile/DevOps teams

Penetration Testing

- Application, API, infrastructure and cloud configuration testing
- Remediation advice, retest options, and executive reporting
- Rules of engagement, permissions and safe-test coordination

Digital Forensics (Advisory and Delivery)

- Forensic acquisition planning, chain-of-custody, and evidence handling
- Triage, analysis, and reporting aligned to legal defensibility
- Lessons-learned and control uplift recommendations

Supply-Chain Security Assurance

- Due diligence checklists, questionnaires, and artefact reviews
- Contractual security clauses and measurable KPIs
- Ongoing assurance plans for critical suppliers

Compliance & Audit Readiness

- Readiness assessments for ISO 27001, Cyber Essentials Plus, NCSC guidance
- Evidence packs, policy mapping and audit interview preparation
- Gap remediation planning and tracking

3. Deliverables

- Security strategy and IA operating model
- Target and current-state cloud security architectures
- Policy suite and standards (drafts and final)
- Risk assessment reports, risk registers and treatment plans
- Secure-by-design requirements, patterns and decision records
- Penetration test plan, findings, retest report and executive summary
- Forensics acquisition plan, analysis report and evidential artifacts (as agreed)
- Supplier assurance reports and action plans
- Compliance gap assessments and audit-ready evidence packs
- Knowledge transfer materials and playbooks

4. Service Benefits (examples)

- Reduces cyber and information risk to critical services
- Improves compliance with UK government security standards
- Accelerates secure delivery and approvals
- Identifies vulnerabilities before they impact operations
- Strengthens protection of sensitive citizen data
- Improves security governance and decision-making
- Enhances supplier and third-party assurance
- Reduces long-term security costs through proactive design

5. Engaging with Evodia

Customer enquiries and Requests for Quotation should be directed to your appointed Bid or Account Manager or by email to info@evodia.co.uk.

Before using our G-Cloud Services, a consultant will work with you to identify the service on the Digital Marketplace that best aligns to your digital transformation objectives.

Once we have agreed the service design our consultant(s) will work with you to develop the Call-Off Contract, during this process, Evodia will confirm the required order details.

Once we have processed your order, Evodia will advise you of the service start date.

6. Terms and Conditions

Please refer to our Terms and Conditions, which are available on our Digital Marketplace service pages.

Further Information

This Service Definition Document should be reviewed in conjunction with:

a. Service Pricing Document
b. Terms & Conditions