Emphasys IT

Your partner for quality IT solutions

GCloud 15 - Lot 3: Cloud Support: Cloud Security

Title	Service Definition
Author	Sunny Tailor
Version	1.0
Date	05/01/2026

Document Administration

Version Control

Version	Date	Author	Reason for Change
1.0	05/01/2026	Sunny Tailor	Baseline

Review

Version	Date	Reviewer	Company	Role
1.0	27/01/2026	Barry Morgan	Emphasys IT	Director

Distribution

Version	Date	Reviewer	Company	Role

Contents

Service Definition

Service Name

Cloud Security

Lot

G-Cloud 15 – Lot 3: Cloud Support

Supplier

Emphasys IT Limited

Service Categories

- Security Services
- Security Strategy
- Security Risk Management
- Security Design
- Security Incident Management
- Security Audit Services
- Security Quality Assurance (QA) and Testing
- Security Other

1. Service Overview

Emphasys IT's Cloud Security service helps organisations design, operate and assure secure cloud platforms and workloads. We provide cloud security support spanning strategy, risk management, secure design, incident management, audit readiness, and security QA/testing.

The service is outcome-led and designed to improve security posture, compliance, resilience and confidence in cloud delivery.

Service Composition and Flexibility

This service is intentionally flexible and can include **any combination of advisory, design, delivery and operational activities**, depending on the Customer's needs.

Activities may include, but are not limited to:

- **Advice and guidance**
  Independent advice, options analysis, recommendations and decision support.
- **Design and architecture**
  Architecture definition, design patterns, standards, and assurance.
- **Process and operating model support**
  Definition or improvement of processes, governance, roles and ways of working.
- **Implementation support**
  Hands-on engineering or configuration activities where explicitly agreed.
- **Operational and support activities**
  Incident support, service management, reporting, optimisation and continuous improvement.

The **specific mix of activities**, level of hands-on involvement, and division of responsibilities is determined by the Customer and confirmed in the Call-Off Order Form.

Unless explicitly stated, services are **not delivered as a fully managed service**, and accountability for production systems and operational decisions remains with the Customer.

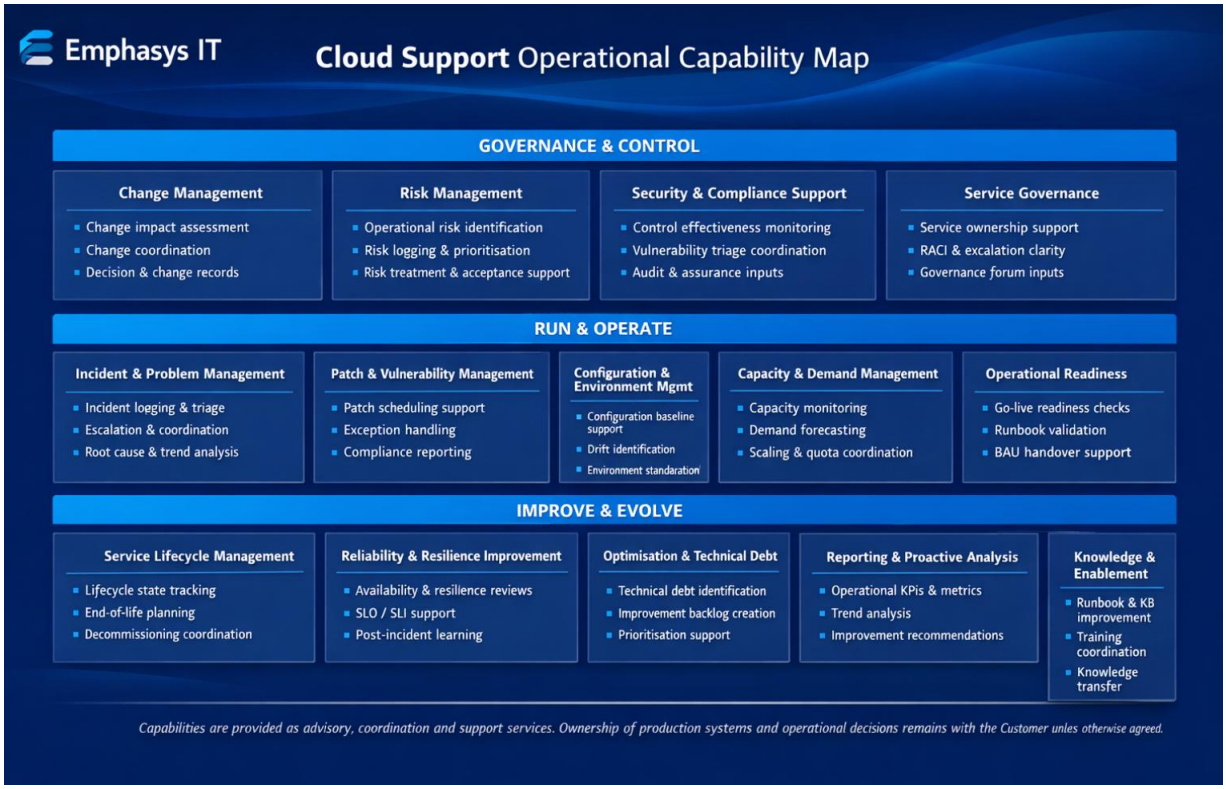
2. Who the Service Is For

This service is suitable for organisations that need to:

- define or improve a cloud security strategy and roadmap
- identify and treat cloud security risks
- establish secure architectures, patterns, and guardrails
- improve security incident readiness and response capability
- prepare for audits and demonstrate control effectiveness
- embed security quality into delivery pipelines and releases

3. Service Scope and Options

Customers can procure one or more of the service categories below. Scope, timelines, and deliverables are agreed in the Call-Off Order Form.



3.1 Security Services

Practical cloud security support across programmes, projects, product teams and operations.

Typical activities:

- security advisory and control interpretation
- guidance for guardrails, baselines, and secure configurations
- backlog/plan shaping and prioritisation of security improvements
- operating model and governance inputs

Typical deliverables:

- security support plan and cadence
- security control mapping and decision logs
- prioritised security backlog/plan
- runbooks and operational procedures (where applicable)

3.2 Security Strategy

Define a clear cloud security strategy aligned to organisational outcomes.

Typical activities:

- identify owners and stakeholders
- strategy workshops and stakeholder alignment
- security principles and standards definition
- roadmap and investment prioritisation
- target operating model inputs

Typical deliverables:

- agreed cloud security strategy artefact(s)
- principles/standards pack
- security roadmap and prioritised initiatives

3.3 Security Risk Management

Identify, assess, and treat security risks and issues across cloud platforms and workloads.

Typical activities:

- identify owners and stakeholders
- risk and issue assessments and risk/issue register creation/maintenance
- threat modelling and control selection
- risk/issue treatment planning and prioritisation
- support for risk acceptance decisions and governance

Typical deliverables:

- cloud security risk/issue register
- threat model outputs and recommendations
- treatment plan and remediation backlog
- governance decision records
- linkage to organisational level risk/issues register

3.4 Security Design

Secure-by-design architecture and patterns for cloud platforms and workloads.

Typical activities:

- identity and access approach and design (least privilege, RBAC, remote access methods, privileged identity management, just in time access, multi-factor authentication)
- network security approach and design (segmentation, boundary controls, defence in depth)
- logging/monitoring and detection approach and design
- secrets/key management approach and design
- data protection and encryption approach and design

Typical deliverables:

- security architecture/design pack
- reference patterns and secure baselines

design recommendations

3.5 Security Incident Management

Improve readiness and support response to security incidents.

Typical activities:

- incident playbooks and escalation paths
- incident triage support (where agreed)
- post-incident reviews and lessons learned
- improvements backlog/plan creation and prioritisation

Typical deliverables:

- incident response playbooks
- escalation routes and communications approach
- PIR (post-incident review) outputs and action backlog

3.6 Security Audit Services

Audit readiness and evidence-based assurance.

Typical activities:

- control reviews and compliance gap assessments
- evidence pack structure and evidence register
- policy/standard alignment checks
- audit support sessions (pre- and during-audit)

Typical deliverables:

- audit readiness report
- evidence register and control mapping

- remediation plan and prioritised actions
- outputs are designed to be audit-ready, traceable to controls and suitable for internal assurance or external audit scrutiny

3.7 Security Quality Assurance (QA) and Testing

Embed security quality into delivery pipelines and releases. This service complements, but does not replace, formal penetration testing or specialist assurance unless explicitly included.

Typical activities:

- identify owners and stakeholders
- secure delivery lifecycle inputs and quality gates
- security acceptance criteria and release assurance
- guidance for CI/CD security checks (code scanning, policy checks)
- vulnerability triage support and remediation planning

Typical deliverables:

- security QA plan and checklists
- acceptance criteria
- vulnerability remediation backlog
- release assurance recommendations

3.8 Other

Additional cloud security support activities can be provided by agreement, such as:

- supplier assurance and technical due diligence
- tabletop exercises and incident simulation workshops
- security coaching for architecture, DevOps and engineering teams
- policy development

4. What's Included

- discovery workshops and stakeholder interviews
- evidence based analysis and recommendations
- documented outputs suitable for governance and approval
- decision logs and traceability
- knowledge transfer sessions and handover packs

5. What's Not Included (Unless agreed)

- implementation/build activities beyond agreed scope
- procurement or licensing of third-party tools
- cloud consumption charges
- penetration testing or specialist assurance beyond agreed scope

6. Customer Responsibilities

The Customer will:

- provide timely access to relevant people/stakeholders, systems, environments, premises (if on-site) and information such as spend, usage and reporting data provide access to cloud management tools and dashboards (where available)
- nominate an authorised representative for decisions and approvals
- provide existing governance and policy standards (if applicable)

7. Onboarding

Delays in onboarding activities may impact delivery timelines and cost and will be managed through change control where necessary.

Onboarding typically includes:

- discovery workshop to confirm outcomes or objectives and constraints
- agreement of scope, deliverables and timelines information and access requirements confirmed

8. Service Levels

Standard support and delivery hours: 09:00–17:00 UK time, Monday–Friday.

Response targets for delivery queries and issues (unless otherwise agreed):

- Critical: 1 hour
- High: 4 hours
- Medium: next business day

Out-of-hours delivery is available by agreement and may be subject to uplifts.

Service Levels apply to delivery communications and support queries and do not constitute guarantees of security services.

9. Security and Compliance

Security is embedded throughout the service:

- least-privilege access and role-based controls for any agreed access
- secure handling of Customer information and credentials
- audit-friendly documentation and decision logs

Where personal data is processed (if required), processing is performed in accordance with UK GDPR and agreed terms.

10. Pricing

Pricing is provided via the published G-Cloud rate card.

- **Time & Materials (T&M):** day-rate pricing for security service, analysis and governance support
- **Retained Support:** monthly retained capacity (days/hours) for continuous security optimisation

Cloud consumption and third party licensing costs are excluded.

11. Deliverables and Acceptance

Deliverables, formats and acceptance criteria are agreed in the Call-Off Order Form. Typical acceptance is based on:

- completion of agreed workshops and evidence gathering
- provision of agreed documents/artefacts and backlogs/plans
- formal review and sign-off by the Customer's authorised representative

12. Exit and Transition

The service is designed to be transferable and avoids supplier lock-in. Exit activities are designed to preserve security posture, audit traceability and operational continuity.

On exit, we will provide:

- final versions of deliverables, dashboards requirements and backlogs/plans
- handover session covering recommendations and next steps
- secure removal of any Supplier access to Customer systems (where applicable)