Cloud/Security Monitoring & Incident Response

Pricing Pack

G-Cloud 15 – Lot 3: Cloud Support Services

Spirit UK Managed Services Ltd

1. Pricing Overview

Cloud Security Monitoring & Incident Response is provided as an ongoing managed support service, priced primarily on a per-user basis, with optional time-bound security response services where additional effort is required.

This approach provides predictable ongoing costs while allowing flexibility for higher-severity or complex security incidents.

All prices are exclusive of VAT.

2. Core Pricing Model (Ongoing Monitoring)

Managed Security Monitoring (SOC-lite)

Item	Unit	Price
Cloud Security Monitoring & Incident Response	Per user / seat / month	£35

Includes:

- Monitoring of supported cloud/security alerts
- Security event triage and investigation
- Incident response support and escalation
- Security reporting and trend analysis

If required we can also provider per service based monitoring but this is subject to survey.

3. Incident Response & Specialist Support (Optional)

Where a security incident requires additional effort beyond standard monitoring, specialist support may be provided as professional services.

Skill-Based Rate Card

Role / Skill Type	Typical Activities	Unit	Price
Security Response Engineer	Incident investigation, containment support	Per day	£900
Senior Security Engineer	Complex incidents, threat analysis	Per day	£1,050
Identity & Access Specialist	Compromised accounts, MFA, conditional access	Per day	£1,000
Incident & Recovery Lead	Coordination, response planning, communications	Per day	£950

Use of these roles is only where required and agreed in advance.

---

4. What's Included

- Continuous monitoring of supported cloud security alerts
- Security event triage and prioritisation
- Incident containment guidance and support
- Escalation to senior engineers where required
- Regular security reporting

---

5. What's Excluded (unless agreed elsewhere)

- Cloud platform consumption costs
- Third-party licences or security tooling
- Penetration testing or red-team exercises
- Formal compliance or certification audits
- Legal, regulatory, or forensic investigation services

---

6. Out-of-Hours Support

- Out-of-hours security response is available by prior agreement
- Charged at 1.5× standard day rates
- Used for critical incidents requiring immediate action

---

7. Invoicing and Payment

- Ongoing monitoring is invoiced monthly in advance
- Incident response services are invoiced in arrears
- Standard payment terms: 30 days from invoice date

---

8. Cost Control and Transparency

- Clear separation between monitoring and incident response costs
- No minimum spend beyond agreed user numbers
- No hidden fees or bundled cloud consumption charges
- Vendor-neutral security recommendations

---

9. Transition and Exit

Customers may:

- Add or remove users with notice
- Transition to alternative support models
- Exit the service in line with agreed notice periods