MUSE CYBER

2026 G-Cloud Service Description

Service Name: Third-Party Cyber Risk Oversight & Monitoring

1. What the service does

The Third-Party Cyber Risk Oversight & Monitoring service provides ongoing, structured support to help organisations maintain visibility and control over cyber security risks arising from third-party suppliers.

The service focuses on periodic assurance, governance, and risk oversight, enabling organisations to track changes in supplier risk posture, validate ongoing controls, and respond proportionately to emerging risks over time.

The service is designed to support organisations in maintaining ongoing visibility and control over third-party cyber risks in a way that aligns with UK Government assurance expectations. It provides structured evidence, risk tracking, and escalation support that can be used to inform internal assurance activities, including those undertaken as part of a GovAssure assessment.

2. Who the service is for

This service is designed for UK public sector organisations that rely on third-party suppliers to deliver digital, operational, or citizen-facing services and require sustained assurance beyond initial onboarding.

The service is suitable for central government departments, arm's-length bodies and executive agencies, police forces, fire and rescue services, NHS Trusts and Integrated Care Systems, local authorities, regulators, and other publicly funded bodies.

It is particularly relevant for organisations that are subject to, or preparing for, formal cyber assurance activities, including those undertaken under the GovAssure framework.

3. What's included

Ongoing risk oversight:

- Maintenance of a third-party cyber risk register
- Periodic review of supplier risk status and criticality
- Tracking of assurance outcomes and known risk issues

Scheduled assurance activities:

- Planned, periodic check-ins with selected suppliers
- Review of updated assurance artefacts (e.g. certifications, policies, incident notifications)
- Validation of progress against previously agreed actions or conditions

Change and escalation support:

- Identification of changes in supplier risk posture
- Support for escalation where risk thresholds are exceeded
- Advice on proportionate response and mitigation options

Reporting and governance:

- Regular summary reporting suitable for senior management or risk committees
- Clear visibility of current supplier risk status and trends
- Support for internal assurance, audit, or regulatory enquiries

Engagement management:

- Named senior consultant responsible for oversight

- Agreed cadence of reviews (e.g. monthly or quarterly)
- Ongoing liaison with nominated organisational stakeholders

4. What's not included

- Continuous or real-time technical monitoring of supplier systems
- Automated scanning or tooling-based monitoring services
- Penetration testing, vulnerability scanning, or red team activity
- Hands-on remediation or implementation within supplier environments
- Legal, regulatory, or audit opinions
- Formal certification, accreditation, or compliance sign-off

5. How the service is delivered

The service is delivered as a retained, time-boxed engagement designed to provide ongoing assurance while remaining proportionate and predictable.

Delivery may be remote, on-site, or hybrid by agreement. Oversight activities are delivered according to an agreed schedule and are structured to minimise burden on both the buying organisation and suppliers.

Overall accountability and assurance judgement are provided by a senior cyber security consultant, supported by appropriately skilled analysts for routine monitoring, reporting, and evidence tracking.

On request, the service includes a structured handover of risk information and artefacts to support transition or internalisation.

6. Security and data handling

Information handled during delivery of this service is managed securely and proportionately in line with UK public sector expectations.

Data collection is limited to what is necessary to support oversight outcomes

and is handled on a need-to-know basis by authorised personnel.

Muse maintains Cyber Essentials Plus certification and operates an ISO/IEC 27001–aligned information security management system. All data handling complies with UK GDPR and relevant public-sector requirements.

7. Pricing approach

The service is priced using transparent day-rate bands reflecting a blended delivery model.

Delivery is led by senior consultants operating at SFIA Levels 5–6, supported by analysts operating at SFIA Levels 3–4 for routine oversight activities. Pricing is based on an agreed allocation of days per period (for example monthly or quarterly).

Travel and on-site costs, where required, are agreed upfront. The service can be directly awarded under G-Cloud.

8. Why Muse

Muse brings a pragmatic, assurance-led approach to third-party cyber risk, grounded in senior practitioner experience and an understanding of public-sector accountability.

The service is designed to provide sustained confidence without unnecessary complexity, helping organisations maintain control over supplier cyber risk in a way that is proportionate, defensible, and aligned to operational reality.