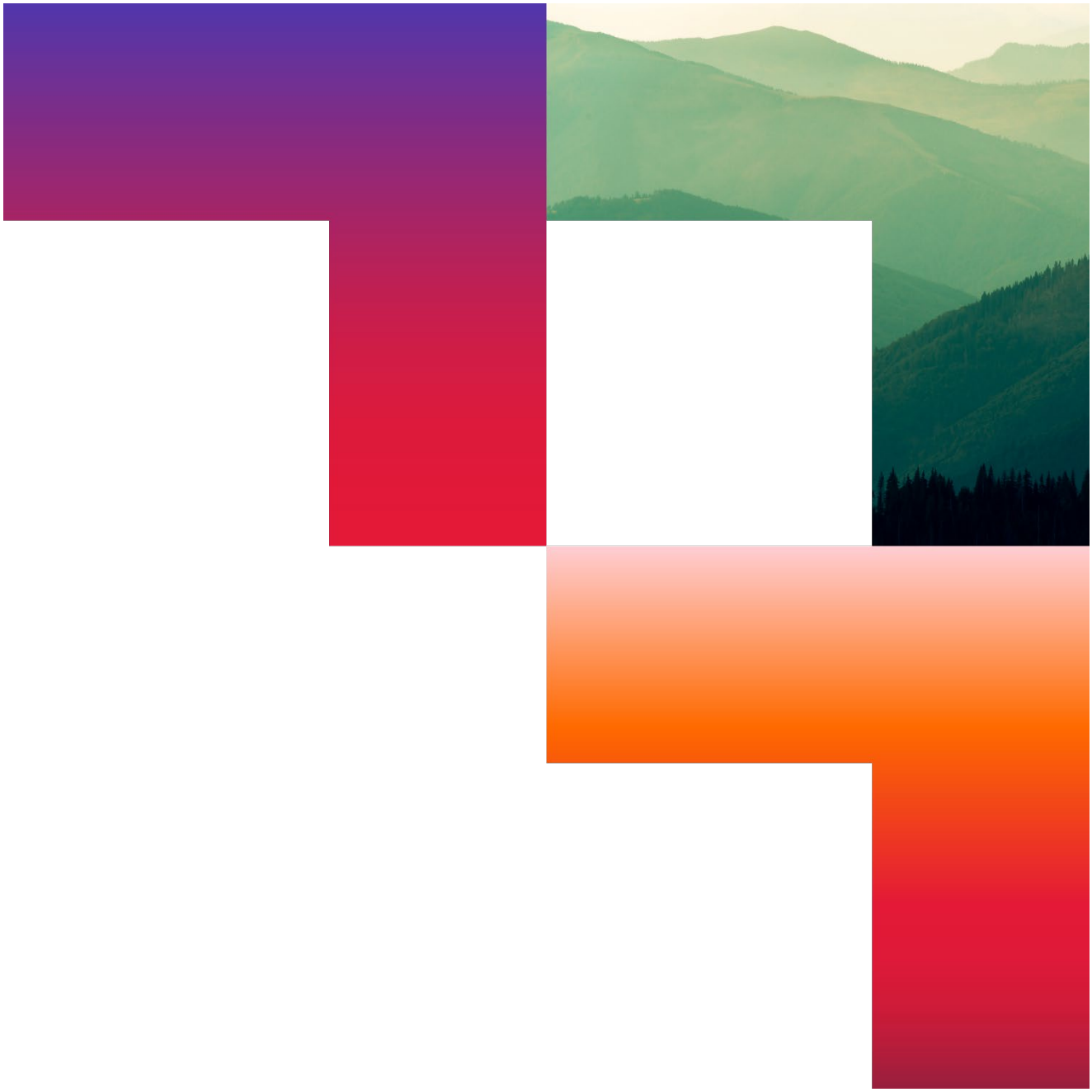


Intelligence led SOC

Contracting Body

30 Jan 2026

Issue 1.0

Table of contents

1. Service Description 4

1.1. Key Service Components 4

1.2. Service Benefits 4

1.3. Proven UK Sovereign Delivery 4

1.4. Intelligence led Security Operations 5

1.5. Advanced Automation and Response Capability 5

1.6. Experience in Complex and High-Risk Environments 5

1.7. Transparent Service Management 5

1.8. Scalable and Sustainable Service 5

1.9. Value for Public Sector Buyers 5

2. Data backup and restore 6

3. Service Continuity 6

3.1. Business Continuity and Disaster Recovery 6

4. Onboarding and Offboarding 6

4.1. Onboarding 6

4.2. Offboarding 6

5. Service constraints 6

6. Service levels 7

7. After sales support 7

8. Technical requirements 7

9. Outage and maintenance management 7

9.1. CGI Hosted 7

9.2. Self-Hosted 7

10. Hosting options and locations 8

10.1. CGI Hosted 8

10.2. Self-Hosted 8

10.3. Locations 8

11. Security 8

11.1. CGI Hosted 8

11.2. Self-Hosted 8

12. Service Pricing and Terms and Conditions 8

12.1. Pricing 8

12.2. Terms and Conditions 8

13. Further information 8

PROPRIETARY AND CONFIDENTIAL 10

Service Definition overview

CGI's Intelligence led Security Operations Centres (SOCs) deliver fully managed, UK based cyber security monitoring and response services. They operate 24/7/365 detection, investigation, and response capabilities tailored to mitigate cyber threats and reduce organisational cyber risk. The services combine advanced threat intelligence, security analytics, and automated response capabilities to protect organisations from cyber incidents including ransomware, account compromise, and advanced persistent threats.

The services can be tailored to meet specific customer demands with options including all services being delivered from CGI infrastructure and using CGI hosted tooling or integrating with your existing security platforms. The services are suitable for organisations operating in regulated environments, including Critical National Infrastructure (CNI) and highly sensitive areas, supporting both IT and OT technology.

Why CGI?

CGI is an established UK supplier of managed cyber security services with a proven capability to deliver secure, resilient, and intelligence led Security Operations Centre (SOC) services for public and private sector organisations, including Critical National Infrastructure (CNI).

1. Service Description

1.1. Key Service Components

The service offered by CGI is highly tailorable to meet your needs. Typically, the service would include the following key components:

- **Protective Monitoring**. Providing an ‘eyes on glass’ monitoring service, with analysts looking at data, logs and alerts from client systems. This can be weekdays only or extend to full 24/7 coverage depending on client need.
- **Incident Handling and Response**. When incidents do occur, our team of experts will conduct stakeholder engagement, reporting and where needed, take remediation actions.
- **Threat Hunting**. Conduct proactive cyber security in the form of Threat Hunting activities, looking for the absence of the normal and/or the presence of the abnormal. To do this, we take intelligence from emerging threats and turn it into actionable investigations, looking to find evidence of compromise beyond traditional IDS alerting or similar detection techniques.
- **Threat Intelligence**. Using a diverse range of intelligence sources, we derive relevant, domain specific information and assess the impact of emerging threats. This threat information is then used to improve and harden networks/systems, deploy new detections, conduct threat hunts or provide awareness/information – all aimed at reducing cyber security risk.
- **Malware and Forensics**. As needed, the team can leverage their skills and experience to piece together an attack or compromise. This work relies on highly skilled analysts, utilising specialist tools and techniques to look for evidence of abnormal actions. The team are also able to perform a level of Malware analytics, helping to understand the intent or source of a suspect piece of code.
- **Vulnerability Scanning**. To avoid security incidents occurring in the first place, the team are able to conduct a level of Vulnerability Scanning. By looking at a system, its components and configuration it is possible to identify potential weak points and recommend mitigations and remediations.
- **Automation and AI**. Where possible, the SOC leverages automation technology to improve triage and response times. The SOC is also able to leverage AI tooling to support event and alert triage, data onboarding and case management.

1.2. Service Benefits

By combining skilled analysts, threat intelligence, automation and artificial intelligence the service delivers a scalable and resilient approach to modern cyber defence. A CGI Intelligence led SOC enables organisations to:

- Detect, respond and contain cyber threats quickly.
- Works with both IT and OT technology.
- Reduce the impact of security incidents.
- Gain visibility of your threat landscape.
- Improve your overall security posture.

1.3. Proven UK Sovereign Delivery

CGI is a proven and trusted supplier of UK Sovereign SOC capabilities. Doing so ensures compliance with UK government security expectations and supports organisations with high assurance requirements. Specifically, our SOC services:

- Are delivered from UK based facilities.
- Security analysts are UK nationals, SC cleared as a minimum, with team members holding DV if required.
- Suitable for regulated environments requiring sovereign control and assured access.

1.4. Intelligence led Security Operations

CGI's SOCs operate using an intelligence-first model, ensuring that detection, investigation, and response activities are driven by current and relevant threat intelligence rather than generic alerting. Threat intelligence is sourced from CGI's global SOC network and specialist open and closed intelligence feeds. This model has the benefits of:

- Improves detection accuracy.
- Reduces false positives.
- Enables earlier identification of emerging threats.
- Aligns monitoring to real-world attacker behaviour.

1.5. Advanced Automation and Response Capability

CGI augments native SIEM and XDR tooling with its AI enabled SOAR platform, enabling:

- Automated alert enrichment and triage.
- Faster investigation of known attack patterns.
- Optional pre-approved automated response actions.

This reduces response times and analyst workload while maintaining customer control over remediation activities.

1.6. Experience in Complex and High-Risk Environments

CGI has extensive experience delivering cyber security services for organisations operating in:

- Critical National Infrastructure.
- Highly regulated industries.
- Large, complex IT and OT environments.

Services are designed to integrate with existing customer platforms, processes, and governance structures.

1.7. Transparent Service Management

CGI provides:

- Dedicated Service Delivery Management.
- Regular service reporting and reviews.
- Clear escalation routes and accountability.

This ensures service performance is measurable, auditable, and continuously improved.

1.8. Scalable and Sustainable Service

The SOC service is designed to:

- Scale with changing threat levels and log volumes.
- Evolve detection coverage automatically as threats change.
- Support long-term service delivery without repeated re-procurement.

1.9. Value for Public Sector Buyers

For G-Cloud buyers, CGI offers:

- A compliant, off-the-shelf managed SOC service.
- UK-sovereign delivery aligned to government security expectations.
- Predictable service outcomes and clear responsibilities.
- Clear reporting and outputs that align with the NCSC and Cabinet Office for seamless onward reporting.

2. Data backup and restore

The requirements for data backup and restoration are informed by regulation or policy and as such would be agreed during contract negotiation.

3. Service Continuity

3.1. Business Continuity and Disaster Recovery

CGI's Intelligence Led SOC capability has been designed from the outset with service resilience in mind. To realise this, the service is delivered out of geographically dispersed locations. Our offices have been fitted with a range of connectivity services and have Business Continuity Plans in place. The BCPs are subject to annual review. CGI UK, as a corporate entity has achieved and retains ISO22301 certification for Business Continuity.

4. Onboarding and Offboarding

4.1. Onboarding

During onboarding, CGI works with customers to understand their business operations, technology stack, and risk profile. A baseline of normal behaviour is established, and customer-specific detection rules are implemented. These rules are designed with the customer to ensure their specific requirements and concerns are addressed. Informed by intelligence, the SOC then works to maintain these detection rules throughout the delivery of the service.

Onboarding also includes detailed discussions on the approach to incident response actions. Where possible, and appropriate, the SOC will work to automate response actions utilising Security Orchestration and Automate Response (SOAR) tooling. The onboarding stage will also include agreement on reporting processes to ensure that relevant organisation policy or regulatory requirements are being met.

4.2. Offboarding

The approach to offboarding will be dependent on the nature of the service that is delivered. Off-boarding is instigated by a client request or after expiration of the service agreement.

4.2.1. Access to data upon exit

For services delivered using CGI hosted systems, any required data will be made available using appropriate media, in line with the data security classification. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any computer or storage device or media that remains part of CGI's estate, with the exception of any data related to a data retention agreement between a client and CGI.

5. Service constraints

CGI will work with you to define and tailor the services to meet your specific requirements. During this definition period, detailed responsibilities will be agreed across the service delivery. Examples of common general constraints are listed below:

- Share the existing internal sponsorship and governance for Information Assurance.
- Assign or appoint a suitably skilled and empowered person to act as the receiving client.
- Provide appropriate access to its policies, processes and standards for the Information Assurance service and other suppliers.
- Provide timely information relating to its business plans, goals and projects.

As a main feature of any Service will necessitate an on-going dialogue with client representatives, the most important responsibility of the Contracting Body is to ensure the timely availability of individuals for fact-finding interviews.

6. Service levels

The SOC service can be tailored to meet customer needs. Whilst we would always recommend 24/7/365 coverage is applied to any 'always on' system, the service can optionally be delivered to reduced hours, such as Monday to Friday. The service can also be tailored in terms of how the team responds to incidents. In some cases, the SOC will be empowered to take immediate response actions, for example shutting down external connectivity in case of confirmed data exfiltration. In other cases, you may want a simple notification service where the SOC would inform you of a potential compromise and await customer direction.

The service offered by CGI is also able to operate across UK Gov security classifications with the environment and technology used to deliver the service tailored to meet your needs.

7. After sales support

The requirements for after sales support would be agreed during contract negotiation.

8. Technical requirements

The technical requirements for the SOC service will vary depending on the type of service selected. For example, if using all CGI hosted tooling there will be a requirement to be able to interface with the log collection technology - which would be as simple as enabling logs to be forwarded to an assigned ingestion point, in an agreed format. In scenarios where tooling is already in place, and the CGI SOC service is to operate on customer tooling, more detailed conversations would be needed to ensure all elements needed to enable the service are in place, for example, having a SIEM, a case management solution would be a minimum with additional tools such as a SOAR application a welcome addition.

9. Outage and maintenance management

9.1. CGI Hosted

Where customers elect to have the SOC service delivered using CGI hosted tooling, CGI assume responsibility for the management of outages of their tooling. All SOC tooling is maintained by a dedicated team of SOC Tooling SMEs who ensure the tools are maintained and patched. The tools have been architected to ensure any planned downtime is kept to a minimum. Where outages do occur, technology is in place to ensure logs are stored and can be ingested once the systems are running again. This ensures that’s any outages do not result in period of no monitoring.

9.2. Self-Hosted

Where the service is being operated from client hosted and owned systems, CGI will work with the customer to establish a greed RACI matrix to ensure all parties understand responsibilities. As needed, CGI are able to provide SOC tooling SMEs to support the customer to maintain their tooling.

10. Hosting options and locations

10.1. CGI Hosted

The SOC service can be delivered as an on premises or in the cloud offering.

10.2. Self-Hosted

CGI SOC services are able to be delivered by utilising client tooling. We would, in effect provide a team of SMEs who would then operate using your existing monitoring tooling, supplemented as needed by our intelligence feeds and platforms. The service can also work in a hybrid model where you existing tooling forwards logs and alerts into CGI hosted tooling to maximise the efficiencies that can be had through the application of our advanced SOAR capabilities.

10.3. Locations

The SOC service, if delivered from a CGI office would be located in either Reading, Chippenham or Bridgend. These facilities already hold a range of UK Gov security accreditation states and connectivity into Government owned networks.

11. Security

11.1. CGI Hosted

All CGI hosted tooling complies with relevant security policy. For example when working with MOD we have built solutions and services that comply with the full extent of Secure by Design (SbD), and Joint Service Publications (JSP) such as JSP 453 and JSP 440 (as well as the relevant DefStans).

11.2. Self-Hosted

The security and integrity of self-hosted systems remain with the customer. CGI team members, if operating the tooling would comply with all necessary security controls and, if needed can advise on how existing controls could be improved.

12. Service Pricing and Terms and Conditions

12.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

12.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

13. Further information

For more information about this or any of our G-Cloud services, please contact us:

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

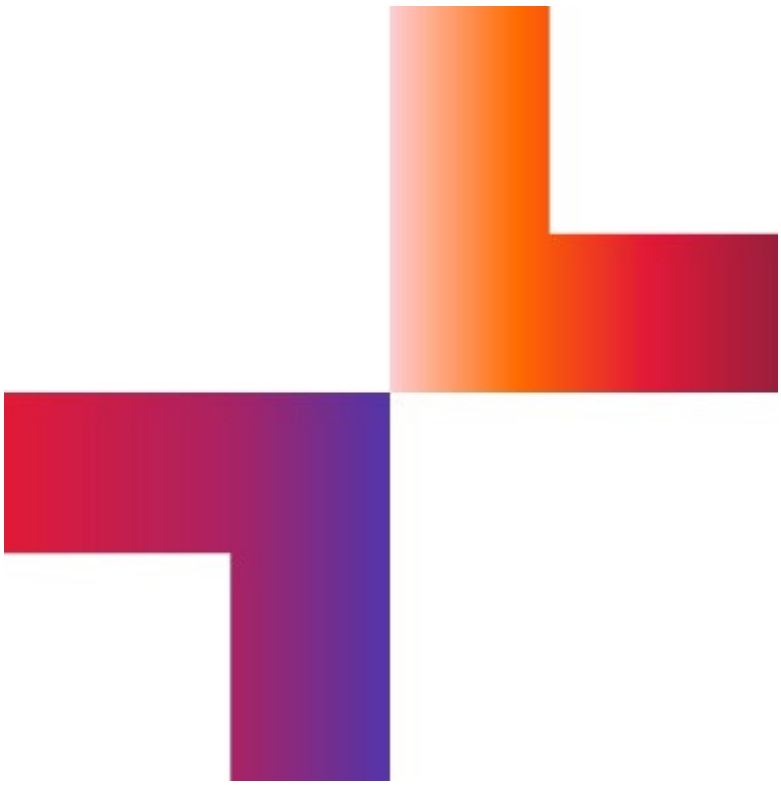
Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765



cgi.com/uk