



DevSecOps Managed Service

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
1.1.	Service Delivery and Approach	4
1.2.	Knowledge Transfer	4
1.3.	Benefits Realisation	4
2.	Data backup and restore	5
3.	Service Continuity	5
4.	Onboarding and Offboarding	6
5.	Service levels	6
5.1.	Service levels management - performance, types and support hours	6
5.2.	Availability and incident responses	8
5.3.	Outage and maintenance management	8
5.4.	Compensation - service credits	8
6.	After sales support	8
7.	Hosting options and locations	8
8.	Security and Information Assurance	9
9.	Service Pricing and Terms and Conditions	9
9.1.	Pricing	9
9.2.	Terms and Conditions	9
10.	Further information	9
PROPRIETARY AND CONFIDENTIAL		10

Service Definition overview

CGI's DevSecOps managed service introduces DevSecOps culture, practices and tools to your organisation. We will work with your existing team in an open and collaborative manner to transfer knowledge, build and help to implement better working practices across all stages in the software development lifecycle.

Why CGI?

CGI has a rich history of collaborating with government agencies, providing them with a deep and comprehensive understanding of their unique IT requirements, challenges, and regulatory constraints specific to the public sector. CGI's comprehensive DevSecOps strategy encompasses all aspects from development to management, ensuring agility and compliance with continuous integration and delivery practices in projects. Security is paramount in government operations, and CGI's services conform to the most stringent security standards, including the Government Security Classifications and GDPR. This guarantees not only increased operational capabilities but also effective protection and safeguarding of sensitive data.

CGI consistently stays ahead in terms of technological advancements, integrating new tools and methodologies to refine service delivery. This means access to the latest innovations in software development and IT operations without the direct investment in research and development. Our services include our innovative DevSecOps, ITIL4 strategies, enhanced through Site Reliability Engineering, FinOps and GreenOps practices.

1. Service Description

DevSecOps is a combination of cultural philosophies, practices and tools that when implemented is proven to vastly improve software quality and provide faster bug fixes when issues are discovered. CGI's DevSecOps managed service consultancy will enable you to expose your organisation's product teams to the benefits of a DevSecOps culture. Continuous horizon scanning of the latest tooling and practices enables CGI to evaluate, recommend and implement cutting-edge approaches to software delivery.

By breaking down silos and promoting a culture of continuous improvement, we will work with your existing product teams in an open and collaborative manner to transfer knowledge, build and help to implement better working practices across all stages in the software development life cycle.

Introducing and optimising automated deployment and release practices to your organisation will reduce system downtime, with potential to reach zero downtime, and ensure reliable and repeatable deployments of your key systems and software.

DevSecOps monitoring approaches enable systems to react to uncommon events, such as peak demands or hardware failure, and automatically recover themselves without user interaction.

CGI advocate continuous testing, baked into the build and deployment pipelines, which enables software bugs to be found and rectified earlier, in turn, delivering higher quality software to your end users.

By introducing security approaches at the earliest feasible opportunity, CGI also promote continuous security scanning of software throughout the build and deployment pipelines to reduce the likelihood of vulnerable software being deployed to your production platforms.

We confirm that this proposition delivers or supports the principles of Cloud services, including NIST definitions and characteristics.

1.1. Service Delivery and Approach

1.1.1. DevSecOps Lifecycle

The DevSecOps lifecycle focuses on combining the classically distinct project and operations phases into a single, product focused, continuous practice. The benefits of which are a shortened development cycle while delivering features, fixes, and updates frequently in close alignment with business objectives. The key stages of the DevSecOps lifecycle are:

- Continuous Development
- Continuous Integration
- Continuous Testing
- Continuous Monitoring
- Continuous Feedback
- Continuous Deployment
- Continuous Operations.

1.2. Knowledge Transfer

In the process of working with us, your organisation will benefit from the knowledge of our engineers by gaining expertise, allowing them to operate more effectively and efficiently, and enabling much higher levels of autonomy.

1.3. Benefits Realisation

1.3.1. Reduce Costs

A large source of issues, and hence costs to your organisation, will be errors resulting from human input in processes that should be automated. Gone should be the days of system administrators manually applying ad-hoc updates to your platform environment, or humans deploying application components by hand. Application

deployment and managing your environment efficiently now requires a high degree of knowledge of processes and tooling to remove as much human input as possible. Our services and knowledge help you identify where and how you can achieve automation of configuration management and deployment.

1.3.2. Automate Everything

In recent years, many excellent tools have emerged that enable your organisation to get very close to 100% automation of your application deployment processes and the platform your application runs on. This kind of automation is essential to implementing continuous delivery, a modern process that enables you to get new features out to your users very shortly after they're available; both users and developers benefit from this quicker feedback cycle. Our DevSecOps engineers have a high degree of knowledge both of the processes and the tools that enable these levels of automation.

1.3.3. Testability

Understanding of modern tooling now enables much more elaborate testing scenarios than previously possible, largely due to the speed at which environments can be constructed in an automated, on-the-fly fashion. Our engineers can help you identify the right tools to construct an environment where you can run integration, acceptance or non-functional test suites upon every code commit. The end result for you is much higher levels of confidence in what you deploy to production. In addition, we will help you design these test environments to mirror production as closely as practicable, including representative data, configurations and access controls, so that issues are identified early and in the right context. We will also embed test automation and quality gates into your CI-CD pipeline so that defects are prevented from progressing downstream, reducing rework and accelerating release cadence. Finally, we support you to establish clear test coverage and non-functional thresholds (for example performance, resilience and security) with transparent reporting, giving delivery teams and stakeholders an evidence-based view of readiness at every release.

1.3.4. Elasticity

With our expertise, you can have elastic, cost effective cloud-based solutions, meaning you only ever pay for what's been consumed. We can enable your environment and applications to scale to meet their current needs, whether that is scaling up during periods of heavy activity or scaling down during quieter periods.

1.3.5. Resilience

In the modern world, users demand high availability of applications and services. Indeed, a large part of an organisation's reputation can now depend on high availability. Being resilient is key to high availability, because even despite everyone's best efforts, at some point, environmental failure is inevitable. We can provide expertise to enable replication of your environment for improved failover, and very importantly, automated disaster recovery solutions to get you back up and running and keep your users happy.

2. Data backup and restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the IA Backup and Restore policies as defined in ISO 27001; any information that has been processed as part of an engagement will be stored securely. Where applicable, this information can then be restored from an appropriate back-up, should the need arise.

3. Service Continuity

CGI will agree appropriate service continuity in accordance with any specific requirements, and any conditions that need to be met.

4. Onboarding and Offboarding

CGI has proven and effective on and off boarding skills, tools and methodologies. We have successfully transitioned numerous Public Sector clients onto Cloud infrastructures and services. CGI has a dedicated team of managers who specialise in transition and who bring to bear considerable previous experience in this area. CGI will apply its standard transition methodology which has been used in all service on- and offboarding's within CGI for many years. The transition process is flexible and can be used for both small and large scale on-boarding requirements.

The approach taken by CGI is to understand the client's requirements and make the transition phase specific to the needs of the client whilst leveraging the experience, lessons learnt and methodology from many years of transition experience.

Service Offboarding is instigated by a client request or after expiration of the service agreement. Deletion of any virtual machine image and data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification. Pricing of this service is dependent on requirements; please contact CGI for details. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any compute or storage device/media that remains part of CGI's estate.

4.1.1. Access to data upon exit

Deletion of any virtual machine image and data will occur in line with the service agreement. 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 levels

5.1. Service levels management - performance, types and support hours

The overall accountability for the relationship with a client lies with CGI's Executive Sponsor and Account Manager, who provide **strategic** governance to the service through working closely with the client's Senior Executive team. Their purpose to ensure that the relationship is healthy, the service is delivering to defined levels, the governance model is working, and best practice is being applied.

At a **tactical** level, CGI's solution is delivered to an agreed set of performance standards backed by a specific Service Level Agreement. A Service Delivery Manager is responsible for overseeing delivery against all service levels and is primarily responsible for ensuring that the service continues to meet client's needs and service levels. They also act as the key single point of contact for discussions concerning strategic issues, additional requirements and gathering information on relevant new products and technologies.

At an **operational** level, the Service Provision Manager (SPM) will also be assigned to manage the day-to-day service. The SPM will be responsible for managing the integration between CGI teams and sub-contractors making sure that any requests for service are directed to the appropriate support consultant and resolved in line with agreed service levels. This model is illustrated in Figure 1.

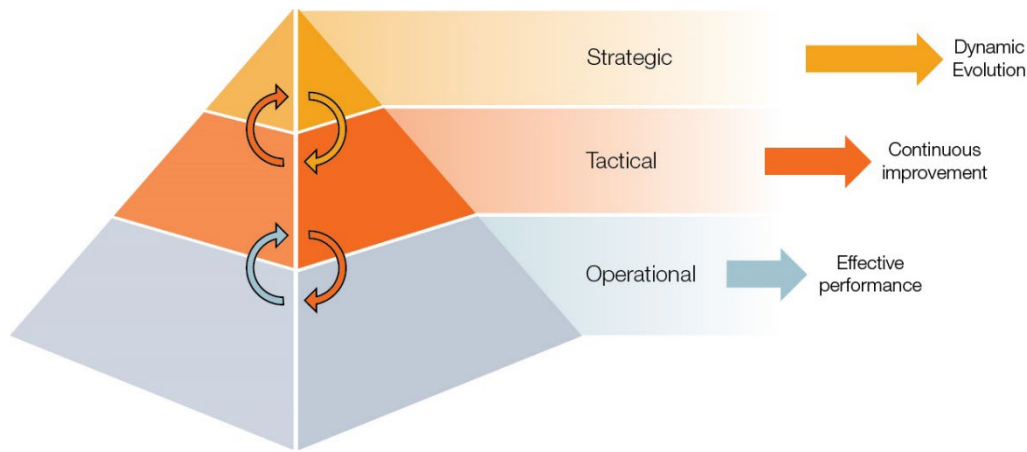


Figure 1 CGI Service Management Model

Service System and Process: CGI's standard IT Service Management system is based on ServiceNow and is aligned to the latest ITIL recommended processes enabling us to drive efficiencies through standardisation, reduce costs and to deliver the same consistently high quality of services to all our clients, big or small, local or global. However, we are flexible, and our AMS teams have experience in using many client and third-party ITSM tools.

Service Reviews and Reporting: Our approach to service delivery means that CGI continually monitors the service provided and reports and discusses this information with the client to provide full visibility of the service being delivered. Regular reports give a summary of the actual support usage and provide details concerning the status of calls, duration of time spent on each call and our performance against the agreed service levels. The reports also provide a picture of how the service is being used and may help to provide early warnings of recurring issues or training needs. Formal service reviews will take place as agreed with the client and the purpose of these reviews is to ensure that the service is at least meeting requirements and also to pick up on immeasurable areas that can lead to potential dissatisfaction and service improvement opportunities.

Continuous Improvement Initiative: Our Service Management team identifies initiatives to improve user experience or provide operational efficiencies throughout the term of the contract starting with the initial application take-on. Where we identify specific areas to improve, we will discuss and prioritise these with the agreement of the client.

The following attributes of our service and variants available will be discussed during the call-off process. CGI will be pleased to discuss client specific constraints and options available.

Attribute	Standard	Optional Variants
Location	UK	Offshore and Nearshore member can be provided should security restrictions permit Welsh language services
Service Hours	Standard Hours Mon to Fri - 08:00 to 18:00	Extended Hours 24x7 including Public Holidays
Application Management Team	CGI's Dedicated or Shared Service Members CGI's Service Management Team	TUPE staff Management of Third Parties
Technology	All commonly used programming languages and software	Support for esoteric software and programming language depending on knowledge transfer
Service Desk	CGI Service Desk	Client or third-party Service Desk

Attribute	Standard	Optional Variants
ITSM Tool	ServiceNow	Client or third party ITSM tool

Table 1 CGI Service parameters

5.2. Availability and incident responses

CGI recognises that the approach to managing the service and relationship with clients is key to the success of our on-going service. CGI is able to offer the comfort that, as well as having a structured methodology, our solution will be delivered to an agreed set of performance standards backed by a specific Service Level Agreement tailored to client requirements, including incident priorities and expected availability, which will be regularly reviewed.

5.3. Outage and maintenance management

CGI will be responsible for ensuring applications are available for use according to the conditions of the Service Level Agreements and in a cost-effective manner. Based on your requirements we will work with all relevant stake holders to analyse, monitor, and report on aspects of the design, implementation, and management of all applications or components which are in-scope of the AMS which affect availability. Planned downtimes (maintenance breaks) will be excluded from the measurement calculations of availability.

5.4. Compensation - service credits

The regime for compensation and service credits will be discussed during the call-off process.

6. After sales support

The overall accountability for the relationship with the client lies with CGI's Executive Sponsor and CGI Account Manager and they provide strategic governance to the service working closely with the client's Senior Executive team. The purpose of this team is to ensure that the relationship is healthy, the service is delivering, the governance model is working, and best practice is being applied.

7. Hosting options and locations

Targets will be as per the relevant cloud platform selected by the supplier from those available - Microsoft Azure, Amazon Web Services, and Oracle Cloud Infrastructure.

The design and delivery of our Application Services offerings is consistent with the principles of the Greening Government ICT Strategy. Scalable, Cloud-based services allow pooling of capacity across multiple clients, reducing overall hardware requirements. These are further reduced through virtualisation, which has delivered up to a 90% reduction in server numbers and power consumption for some of our services. We select modern, energy efficient servers, storage and network hardware and have also invested heavily in improving the energy efficiency of our data centres. This includes initiatives such as free air cooling, aisle containment, power supply upgrades, lighting controls and power management and monitoring software. In the UK, electricity for our data centres is sourced from renewables, which is also the case for many of our third-party hosting providers. We closely manage the impact of IT hardware throughout its lifecycle, aiming to optimise refresh cycles to balance in-use carbon savings of newer, more efficient hardware against the carbon impact of its manufacture. At end of life, we also ensure responsible disposal through resale or recycling of old hardware wherever possible. Our sustainability performance has won widespread recognition, including our listing on the Carbon Disclosure Leadership Index for four consecutive years and our certification under the Carbon Trust Standard.

8. Security and Information Assurance

By embedding security into all practices right from the vulnerabilities within a code base are more likely to be identified and at an earlier stage within the software development life cycle leading to safer code being deployed to production environments and ultimately providing greater protection to your business.

CGI uses our Management Foundation including our Integrated Management System (IMS) for information assurance. These IMS processes are independently certified to BS/EN/ISO 9001:2008.

CGI is committed to retaining our current range of UK-based certifications and will extend these to meet client expectations as required.

The CGI Management Foundation design allows incorporation of best practice from across all of our Public Sector and Commercial engagements.

Our accreditations include:

- ISO9001, ISO27001 and ISO20000
- ISO/IEC 27001:2005 Audit and Certification SSAE 16/ISAE 3402 Attestation
- E.U. Data Protection Directive - (95/46/EC).

All information is held at the appropriate security level for the service. CGI hosted services can be provided at any level defined in the new Government Security Classification (GSC) policy with the appropriate assurance.

9. Service Pricing and Terms and Conditions

9.1. Pricing

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

9.2. Terms and Conditions

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

10. Further information

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

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.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary 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 contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

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

