



Cyber Security Advisory Services

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
2.	Data Backup and Restore	4
3.	Service Continuity	4
4.	Onboarding and Offboarding	5
4.1.	On-boarding	5
4.2.	Off-boarding	5
5.	Service Constraints	5
6.	Service Levels	5
7.	Hosting Options and Locations	5
8.	Security	6
9.	Service Pricing and Terms and Conditions	6
9.1.	Pricing	6
9.2.	Terms and Conditions	6
10.	Further Information	7
PROPRIETARY AND CONFIDENTIAL		8

Service Definition Overview

Organisations are increasingly having to defend against security threats from data leaks, hackers, state-sponsored organisations, and more. This includes ransomware and data extortion, supply chain compromise, vulnerability exploitation and identity-based attacks across cloud and hybrid environments. Geopolitical instability amplifies these threats to the business.

CGI Cyber security advisory services help organisations to assess, design and build holistic and balanced cyber security and risk management strategies through comprehensive risk management that seeks to protect the business, while fostering agility and innovation. We provide pragmatic, risk-driven advice and prioritised roadmaps that are proportionate and implementable.

Effective security is central to how we meet many of these challenges, particularly in Government. It is vital for public confidence and for the efficient, effective, and safe conduct of public business. We offer a comprehensive range of cyber security advisory and assurance services, designed to help organisations understand, identify, and manage the risks involved with developing, implementing, and maintaining digital solutions, including cloud and hybrid solutions. This includes aligning security controls to recognised good practice (e.g. NCSC guidance, ISO/IEC 27001 and NIST-aligned approaches) and data protection requirements.

Why CGI?

CGI recognises the Government's need to address the identified challenges and we provide a wide range of services within G-Cloud and the Digital Marketplace more widely. As one of the largest security practices in the UK our experience is based on over 40-years of working as a trusted advisor with central and local government and commercial organisations. We combine deep cyber security expertise with practical delivery experience to ensure recommendations are implementable and aligned to operational realities.

Coverage of the complete spectrum of security requirements has been provided using specialist facilities, including a dedicated innovation lab, and we are supported by three accredited security certification facilities, one in the US, one in the UK and one in Canada. This breadth enables us to draw on proven methods, accelerators and multidisciplinary specialists to support advisory, assurance and improvement programmes.

CGI has invested heavily in capabilities and infrastructure to support the Public Sector work it undertakes and CGI has a dedicated Security Directorate who maintain our facilities, clearances, accredited infrastructure, interconnections with government networks and the certification of our corporate infrastructure against ISO/IEC 27001. Our security and assurance capability is underpinned by established governance, risk management and security-by-design practices, with ISO/IEC 27001 certified corporate infrastructure supporting secure delivery.

1. Service Description

CGI have conducted extensive research into the security implications and requirements of cloud and hybrid services and have developed our cyber security advisory services to help clients to understand both the security risks and the business benefits of digital transformation, in a measured and objective manner.

Our Cyber security Advisory services help you prepare for the digital realities of today and the future by taking a realistic, risk-driven approach and acting pragmatically.

- Risk Consulting - Providing risk management, as well as audit and internal control consulting by bringing strong methodological expertise and experience.
- Cybersecurity Consulting - Providing advice and expertise in areas including resilience and business continuity planning, crisis and incident preparedness and privacy advisory.
- Cybersecurity & Risk Mitigation Solutions - Assisting clients to define and prioritise controls and solution options to address their risk mitigation plans, including domain areas such as identity and access management, threat management including specialised processes, solutions, and services, and information protection. This includes support for cloud and hybrid security design, third-party/supply chain risk, and secure operating models.
- Digitisation of Control Functions - Implementation of solutions allowing for the seamless integration of control frameworks (such as ISO 2700x/31000, COSO, COBIT, NIST), policies, and regulations that govern the organisation.
- Auditing and Assurance Support - Defining action plans and monitoring their implementation; our control capabilities encompass various methods (such as IIA), including coordination and oversight of technical controls like penetration testing.

They also bring business expertise, best practices and accelerators, such as maturity and classification models, blueprints and reference architectures, integration templates, and operating and governance models.

CGI delivers information security assurance at a variety of security levels to meet the security risk appetite of the organisation. CGI can assist clients in technology selection, delivery, and operations to defend against advanced threats. We tailor our advice to your operating context and risk appetite, focusing on recommendations that are practical to implement and sustain.

CGI provides cyber security advisory and assurance services that enable clients to benefit from our knowledge of commercial, technical, and regulatory perspectives and implement security from Board level policies through to operational level security standards. Our services help protect your infrastructure and services, shorten the time to introduce new or changed digital services and reduce the risks involved with implementing these services.

Our services provide an inclusive approach to the assessment of risk, to ensure that cloud, platform and third-party offerings (whether our own or those provided to our clients by other providers) will conform to clients' specific information security and regulatory requirements.

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 / 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

4.1. On-boarding

For Specialist Cloud Services, CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services, CGI understands the client's requirements and make on-boarding specific to these needs, using the experience, lessons learnt and methodology from many years of public sector transition experience, we can quickly align to client joiners, movers and leavers policies and ensure that we have appropriately cleared staff for every engagement.

4.2. Off-boarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

4.2.1. 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 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 overall accountability for the relationship with the client lies with CGI's Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

7. Hosting Options and Locations

CGI has a network of 21 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes

this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

8. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognised industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organisation to protect information assets, technologies, facilities, and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organisational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

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

