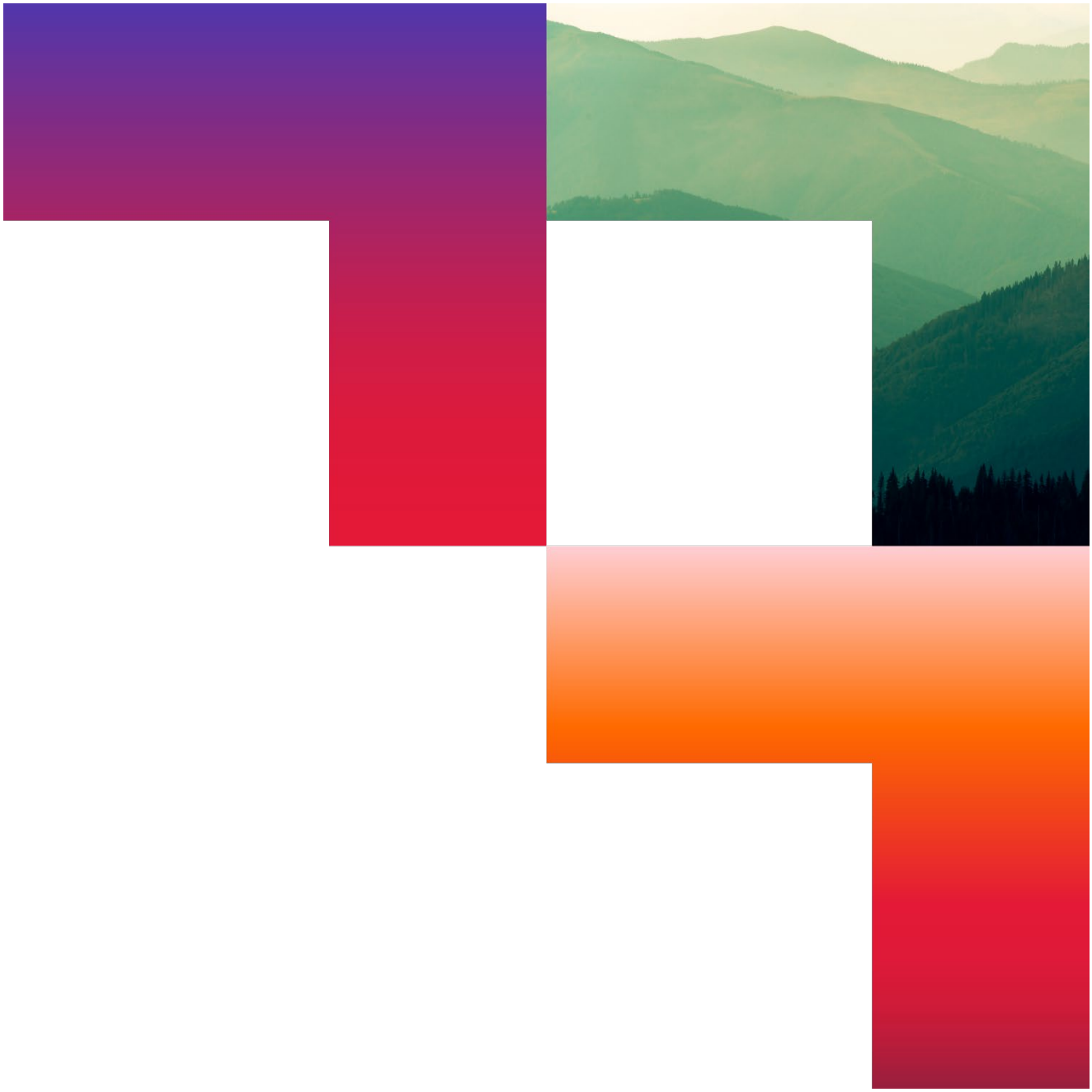


Secure by Design

Contracting body

30 Jan 2026

Issue 2.0

Table of contents

1. Service Description 4

1.1. CGI's SbD Delivery Approach 4

1.2. How the Cyber Strategic Approach Delivers Secure by Design 6

2. Data backup and restore 7

3. Service Continuity 7

4. Onboarding and Offboarding 7

4.1. Onboarding 7

4.2. Offboarding 8

5. Service constraints 8

6. Service levels 9

7. Hosting options and locations 9

8. Security 9

9. Service Pricing and Terms and Conditions 10

9.1. Pricing 10

9.2. Terms and Conditions 10

10. Further information 10

PROPRIETARY AND CONFIDENTIAL 11

Service Definition overview

Security threats are increasing in scale, sophistication and impact, while digital services have become mission-critical to public sector outcomes. Secure by Design (SbD) is no longer optional, it is a foundational requirement for delivering trusted, resilient and cost-effective digital services.

CGI's Secure by Design service embeds security from concept through to decommissioning, ensuring systems are resilient to compromise, easier to detect and respond to, and aligned to government risk appetite and policy.

Our approach moves security from a compliance activity to a delivery enabler, helping organisations:

- Reduce delivery and operational risk
- Achieve assurance faster
- Avoid costly remediation
- Operate services securely throughout their lifecycle.

Backed by over 45 years of UK public sector delivery and deep cyber expertise, CGI provides Secure by Design as a repeatable, assured and scalable service aligned to HMG, MOD and NCSC principles.

Why CGI?

CGI is one of the UK's most experienced providers of Secure by Design services, supporting government departments, defence, critical national infrastructure and regulated industries.

Our differentiators include:

- **Proven Public Sector Delivery**: Over four decades delivering complex, high-assurance systems across central government, defence and national infrastructure.
- **Whole-Life Secure by Design**: Security embedded across design, build, operate and decommission, not limited to early lifecycle assurance.
- **Integrated Cyber Capability**: In-house expertise across architecture, engineering, testing, operations, threat intelligence and incident response.
- **Recognised Assurance and Accreditation**: Including Cyber Security Supplier to Government, CHECK-aligned penetration testing, ISO/IEC 27001:2022, ISO/IEC 27701:2019 and Cyber Essentials Plus.
- **Delivery at Pace**: Secure by Design aligned to Agile, Waterfall and Hybrid delivery models, enabling rapid delivery without sacrificing assurance.

1. Service Description

CGI's Secure by Design (SbD) service enables public sector organisations to design, deliver and operate digital services that are secure, resilient and trustworthy by default. Security is embedded from the earliest stages of service conception and maintained continuously throughout the service lifecycle, ensuring services remain fit for purpose as threats, technologies and business requirements evolve. Secure by Design is a principle-led approach adopted across UK Central Government, Defence and other regulated sectors, and CGI applies these principles pragmatically so that security enables delivery outcomes rather than constraining them.

CGI delivers Secure by Design as a managed, outcome-focused capability that integrates people, processes and technology. Our service brings together advisory, engineering and operational security expertise to ensure security is designed into services from the outset rather than applied retrospectively. This approach supports the delivery of cloud-native and hybrid services, legacy modernisation programmes and the development of new digital platforms and mission-critical systems, while maintaining alignment with government security expectations.

Secure by Design is delivered by CGI as a whole-life service, spanning discovery, design, build, operation and decommissioning. CGI works collaboratively with clients to understand business objectives, risk appetite and data sensitivity, using this insight to define proportionate security architectures, controls and assurance activities aligned to the criticality of the service. Modern security architectures and engineering approaches are applied throughout delivery, including identity led and Zero Trust principles, secure cloud and hybrid architectures and DevSecOps practices that integrate automated security controls into delivery pipelines. Security and privacy controls are designed together to protect data flows across complex ecosystems without compromising usability or performance.

A risk-driven and proportionate approach underpins all Secure by Design activities. CGI works closely with clients and risk owners to identify threats and vulnerabilities, assess risk and define controls that provide clear, evidence-based assurance to senior stakeholders. Secure by Design continues throughout live service operation, supported by CGI's wider cyber and managed security capabilities, ensuring controls remain effective as services evolve and the threat landscape changes. The service is aligned to Secure by Design principles defined by HMG, the Ministry of Defence and the National Cyber Security Centre, and is delivered across Agile, Waterfall and Hybrid delivery models to ensure consistent, assured security outcomes without slowing delivery.

1.1. CGI's SbD Delivery Approach

CGI has extensive experience delivering Secure by Design in alignment with the HMG 10 Secure by Design principles, the NCSC 5 outcomes and the MOD 7 principles. Our approach to solution creation and security, articulated through the CGI Cyber Strategic Approach, enables consistent alignment to these frameworks while remaining adaptable to client context and delivery models.

Principle	HMG	MOD	NCSC
1	Create responsibility for cyber security risk	Understand and Define Context	Establish the context
2	Source secure technology products	Plan the Security Activities	Making compromise difficult
3	Adopt a risk driven approach	Implement Continuous Risk Management	Making disruption difficult
4	Design usable security controls	Define Security Controls	Making compromise detection easier
5	Build in detect and respond security	Engage and Manage the Supply Chain	Reducing the impact of compromise

Principle	HMG	MOD	NCSC
6	Design flexible architectures	Assure, Verify and Test	
7	Minimise the attack surface	Enable Through Life Management	
8	Defend in depth	-	
9	Embed continuous assurance	-	
10	Make changes securely	-	

Table 1 HMG, MOD and NCSC Principles

Figure 1 CGI Cyber Strategic Approach, which has been developed and refined over several years to support the secure delivery of complex client outcomes.

Figure 1 CGI Cyber Strategic Approach

The Cyber Strategic Approach structures Secure by Design activities across three integrated domains, ensuring consistency, assurance and adaptability across the service lifecycle. CGI developed the strategic approach over several years and iterations, to deliver successes securely to our clients. The strategy is divided into 3 areas:

- **Comprehensive protection**: Providing end-to-end, multi-layered cyber security solutions that cover all aspects of your business.
- **Transformative solutions**: Cyber security solutions designed to support rapid or large-scale transformation, helping clients to explore new digital opportunities.
- **Active partnership**: Our cyber team of industry leaders doesn't just follow standards; we proactively engage with our customers and shape critical frameworks, ensuring their business stays ahead.

At the centre of the strategy are CGI's core values of Innovation, Resilience and Privacy, which underpin all Secure by Design activities.

Principle	HMG	MOD	NCSC	CGI Cyber Strategy Alignment
1	Create responsibility for cyber security risk	Understand and define context	Establish the context	**Active Partnership**
2	Source secure technology products	Plan the security activities	Making compromise difficult	**Comprehensive Protection**
3	Adopt a risk-driven approach	Implement continuous risk management	Making disruption difficult	**Active Partnership**
4	Design usable security controls	Define security controls	Making compromise detection easier	**Comprehensive Protection**

5	Build in detect and respond security	Engage and manage the supply chain	Reducing the impact of compromise	**Comprehensive Protection → Active Partnership**
6	Design flexible architectures	Assure, verify and test	–	**Transformative Solutions**
7	Minimise the attack surface	Enable through-life management	–	**Comprehensive Protection → Transformative Solutions**
8	Defend in depth	–	–	**Comprehensive Protection**
9	Embed continuous assurance	–	–	**Transformative Solutions**
10	Make changes securely	–	–	**Transformative Solutions**

Table 2 - CGI Principles Mapping

1.2. How the Cyber Strategic Approach Delivers Secure by Design

The CGI Cyber Strategic Approach provides a practical framework for delivering Secure by Design by embedding security across three mutually reinforcing domains: Comprehensive Protection, Active Partnership and Transformative Solutions.

- **Comprehensive Protection** enables Secure by Design principles that focus on prevention and resilience. It ensures that security is built into services through the sourcing of secure technologies, the design of usable and layered security controls, the minimisation of attack surfaces and the application of defence-in-depth. These measures collectively make compromise and disruption significantly more difficult.
- **Active Partnership** underpins Secure by Design principles that require shared ownership and collaboration. By working closely with risk owners, delivery teams and suppliers, CGI ensures that cyber risk is clearly understood, continuously managed and governed effectively throughout the service lifecycle. This collaborative approach ensures security decisions remain aligned to business objectives and risk appetite.
- **Transformative Solutions** enables Secure by Design through change. Flexible architectures, continuous assurance and secure change management ensure that services can evolve, scale and modernise securely without introducing unmanaged risk, supporting innovation while maintaining trust and resilience.

Together, these three domains ensure Secure by Design is not a one-time activity, but a sustained, practical and business-aligned capability embedded across delivery and operations.

To assess risk comprehensively, CGI provides services covering threat and risk management, governance and compliance, security strategy, maturity assessment and assurance. The insights generated through these activities inform the design of secure architectures and lifecycle controls, secure engineering practices and technology selection, as well as structured test and assurance activities aligned to service criticality.

The Protect phase of the strategy represents the core delivery domain, encompassing infrastructure, solution, security, development, testing, data and service architecture. Intelligence gathered during risk assessment is used to design and implement proportionate technical and security controls, followed by secure build, configuration, testing and assurance. Testing activities include penetration testing, functional and non-functional testing, secure code testing and security assurance testing, ensuring the solution is secure as designed and ready for operation.

Secure by Design continues throughout live service operation. CGI supports clients to operate services with confidence through ongoing cyber threat intelligence, security operations integration, incident response and forensic readiness. This ensures services remain secure, resilient and responsive as the threat landscape and operational requirements evolve.

Secure by Design is an industry-recognised approach that moves beyond traditional compliance-driven security models. It enables organisations to balance security, performance, usability and functionality, provides clear evidence to risk owners that controls operate as intended, and ensures security controls are maintained and

adapted over time. This ultimately supports the delivery of secure digital services that are cost-effective to operate and maintain.

CGI has significant experience delivering Secure by Design under both HMG and MOD methodologies. By aligning our approach to client delivery models, whether Agile or more traditional Waterfall, CGI consistently demonstrates the ability to adapt at pace and support clients in responding effectively to an evolving threat landscape. Our Secure by Design capability enables scalable delivery, assurance and resourcing aligned to client needs.

2. Data backup and restore

CGI delivers data backup and restore as an integral component of its Secure by Design approach, ensuring that resilience, availability and recoverability are designed into services from the outset. Backup and restore arrangements are defined early in the service lifecycle based on business criticality, data sensitivity and risk appetite, and are maintained throughout the operational life of the service.

Backup and restore activities are implemented in accordance with client-specific requirements and in compliance with the Information Assurance backup and restore controls defined in ISO/IEC 27001. All information processed as part of an engagement is protected using proportionate technical and organisational security controls, ensuring confidentiality, integrity and availability are maintained at all times.

CGI designs backup solutions to minimise the impact of compromise or disruption, incorporating secure storage, segregation of duties, access controls and encryption aligned to data classification. Restore capabilities are tested and assured as part of service assurance activities to provide confidence that data can be recovered within agreed recovery objectives should an incident occur.

As part of CGI's whole-life Secure by Design service, backup and restore controls are regularly reviewed and adapted to reflect changes in the service, threat landscape or regulatory requirements. This ensures that recovery capabilities remain effective, auditable and aligned to the client's operational and security objectives, supporting continued service resilience and trust.

3. Service Continuity

Service continuity is embedded within CGI's Secure by Design approach to ensure that digital services remain resilient, available and trustworthy throughout development, transformation and live operation. Continuity requirements are considered from the earliest stages of service design and are aligned to the client's business objectives; risk appetite and the criticality of the service being delivered.

CGI works collaboratively with clients to define proportionate continuity controls that protect the confidentiality, integrity and availability of services and data. These controls are designed to reduce the likelihood and impact of disruption, whether caused by cyber incidents, system failures or operational events, and are integrated into service architecture, delivery and operational processes.

As part of Secure by Design, service continuity arrangements are assured through structured testing and review activities, providing confidence that services can be recovered within agreed objectives in the event of an incident. Continuity controls are maintained and adapted throughout the service lifecycle to reflect changes in the service, operating environment or threat landscape, ensuring ongoing resilience and alignment with Secure by Design principles.

4. Onboarding and Offboarding

4.1. Onboarding

Onboarding is delivered as a core component of CGI's Secure by Design approach, ensuring that security, assurance and operational controls are established from the outset of the engagement. CGI engages directly

with clients to confirm and agree the scope of requirements in advance of service commencement, working collaboratively with stakeholders to understand business outcomes, delivery constraints and security expectations.

As part of Secure by Design onboarding, CGI works with clients to understand risk appetite, data sensitivity and regulatory requirements, using this insight to define proportionate security controls and assurance activities. This ensures that access, environments and delivery processes are established securely and in alignment with the service's criticality and threat profile.

CGI's onboarding approach draws on extensive public sector transition experience and aligns to client joiner, mover and leaver processes. Security clearance, identity and access management controls are applied in line with client policy and Secure by Design principles, ensuring that only authorised and appropriately cleared personnel are granted access to systems, data and environments. This provides a controlled, auditable and secure transition into service delivery.

4.2. Offboarding

Offboarding is delivered as part of CGI's whole-life Secure by Design service and is initiated either at the client's request or on expiry of the service agreement. CGI works with clients to ensure that offboarding activities are planned, controlled and executed securely, minimising risk and maintaining service integrity throughout the transition or exit process.

Secure by Design offboarding ensures that access is withdrawn in a timely and controlled manner, systems are decommissioned securely, and residual risks are identified and managed. Offboarding activities are aligned to contractual, regulatory and assurance requirements to ensure a secure and orderly exit.

4.2.1. Access to data upon exit

Access to data upon exit is managed in accordance with Secure by Design principles, ensuring confidentiality, integrity and availability are maintained throughout the exit process. Deletion of virtual machine images, environments and data is carried out in line with the service agreement and data classification requirements. Where required, client data is securely extracted and made available using appropriate, approved media and transfer mechanisms.

Following client confirmation that data has been successfully recovered, CGI securely purges and destroys all remaining client data from systems, storage devices and media within CGI's estate, except where retention is required under an agreed data retention arrangement. These activities are performed using controlled and auditable processes to provide assurance that data has been handled securely and in compliance with contractual and regulatory obligations.

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

CGI works collaboratively with clients to define and tailor Secure by Design services to meet specific business, security and delivery requirements. During the initial service definition period, roles, responsibilities and accountabilities are agreed to ensure that Secure by Design controls are implemented effectively and proportionately throughout the service lifecycle.

Secure by Design operates on a shared responsibility model. Effective delivery is dependent on the client providing appropriate sponsorship, governance and risk ownership for information assurance and cyber security. This includes the appointment of a suitably skilled and empowered client representative to act as the receiving authority for Secure by Design activities and assurance outcomes.

To enable proportionate and effective security controls, CGI requires timely access to relevant client policies, processes and standards relating to information assurance, cyber security and delivery governance. Where third-party suppliers are involved, collaboration and information sharing are required to ensure Secure by Design principles are applied consistently across the service and supply chain.

CGI also relies on the provision of timely and accurate information relating to the client's business plans, objectives and delivery timelines. This enables Secure by Design activities to be aligned to business priorities and supports informed risk-based decision-making.

As Secure by Design is inherently collaborative, ongoing engagement with client stakeholders is essential. The Contracting Body is responsible for ensuring the timely availability of appropriate personnel for workshops, fact-finding activities and assurance discussions. This enables CGI to maintain effective communication, deliver assurance at pace and ensure Secure by Design outcomes are achieved without unnecessary delay.

7. Hosting options and locations

Hosting options and delivery locations are considered as part of CGI's Secure by Design approach to ensure that security, resilience, assurance and data protection requirements are addressed from the outset. CGI works collaboratively with clients to define hosting and location arrangements that are proportionate to the sensitivity, classification and criticality of the service and the data being processed.

CGI has a network of offices across the United Kingdom and Northern Ireland, enabling services to be delivered securely by UK-based personnel operating as hybrid workers. Where client requirements mandate physical presence, such as for higher assurance environments or operational integration, CGI's distributed office network enables members to work on client sites in a secure and controlled manner.

Hosting and location decisions are informed by risk assessment, regulatory obligations and government policy, including data residency and sovereignty requirements. These considerations are agreed during contract negotiation and service design to ensure alignment with Secure by Design principles, providing confidence that services are delivered from appropriate locations using secure facilities and working practices throughout the service lifecycle.

8. Security

Security is embedded within all CGI services through our Enterprise Security Management Framework (ESMF), which underpins CGI's Secure by Design approach. The ESMF is aligned to recognised international standards and regulatory frameworks, including ISO/IEC 27001, ISO/IEC 27701, NIST, COBIT, CIS, CCPA and GDPR, and provides a consistent, risk-based framework for protecting information assets, technologies, facilities and personnel across the global organisation.

The ESMF is supported by CGI's security and privacy policies, standards and controls, collectively referred to as the CGI Security Baseline. This baseline defines the minimum level of security required for all CGI services, including cloud-based services, and is implemented through CGI's delivery processes, operational practices,

service offerings and interactions with third parties acting on behalf of CGI. This ensures that Secure by Design principles are applied consistently across delivery, operations and the supply chain.

Technical and organisational security measures are defined and applied using a risk-based approach that considers the nature, scope, context and purpose of processing, as well as the potential impact on the confidentiality, integrity and availability of information. Where CGI acts as a data controller or data processor, this approach also considers risks to the rights and freedoms of individuals, ensuring that security and privacy controls are proportionate, effective and aligned to regulatory requirements.

CGI's Security Baseline represents the minimum standard applied to all services; however, Secure by Design recognises that different services carry different levels of risk. Where services involve higher levels of sensitivity, regulatory obligations or business criticality, CGI works with clients to define and implement enhanced security and privacy controls. These additional measures are documented within the contracted service and provide clear, auditable assurance aligned to client risk appetite and Secure by Design outcomes.

Security controls are maintained and reviewed throughout the service lifecycle to ensure they remain effective as services evolve and the threat landscape changes. This whole-life approach ensures that security is not treated as a one-off compliance activity but as an integral and continually assured component of service delivery.

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 2.0 on behalf of CGI by the following authorised representative:

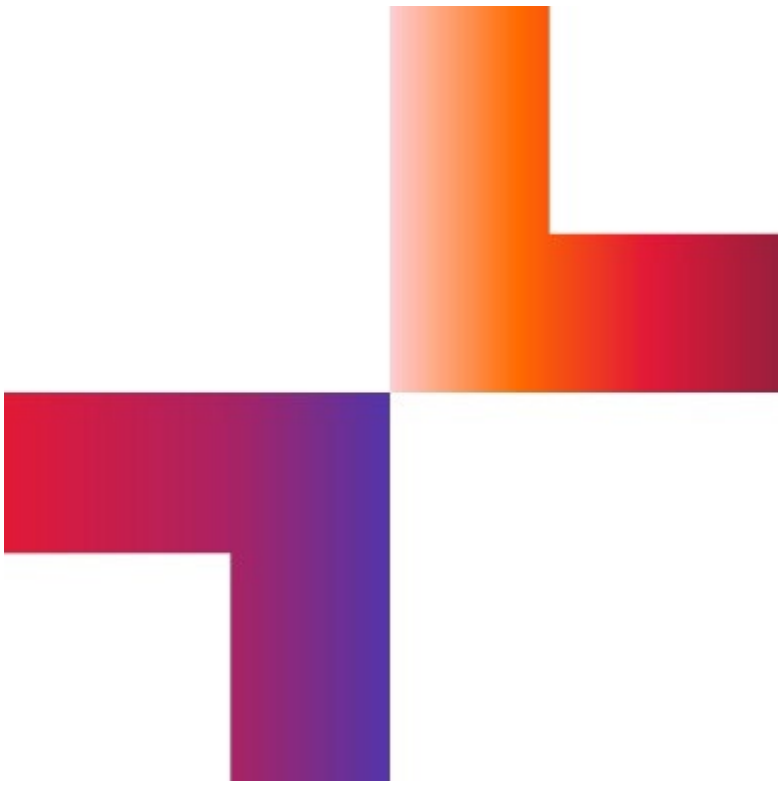
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk