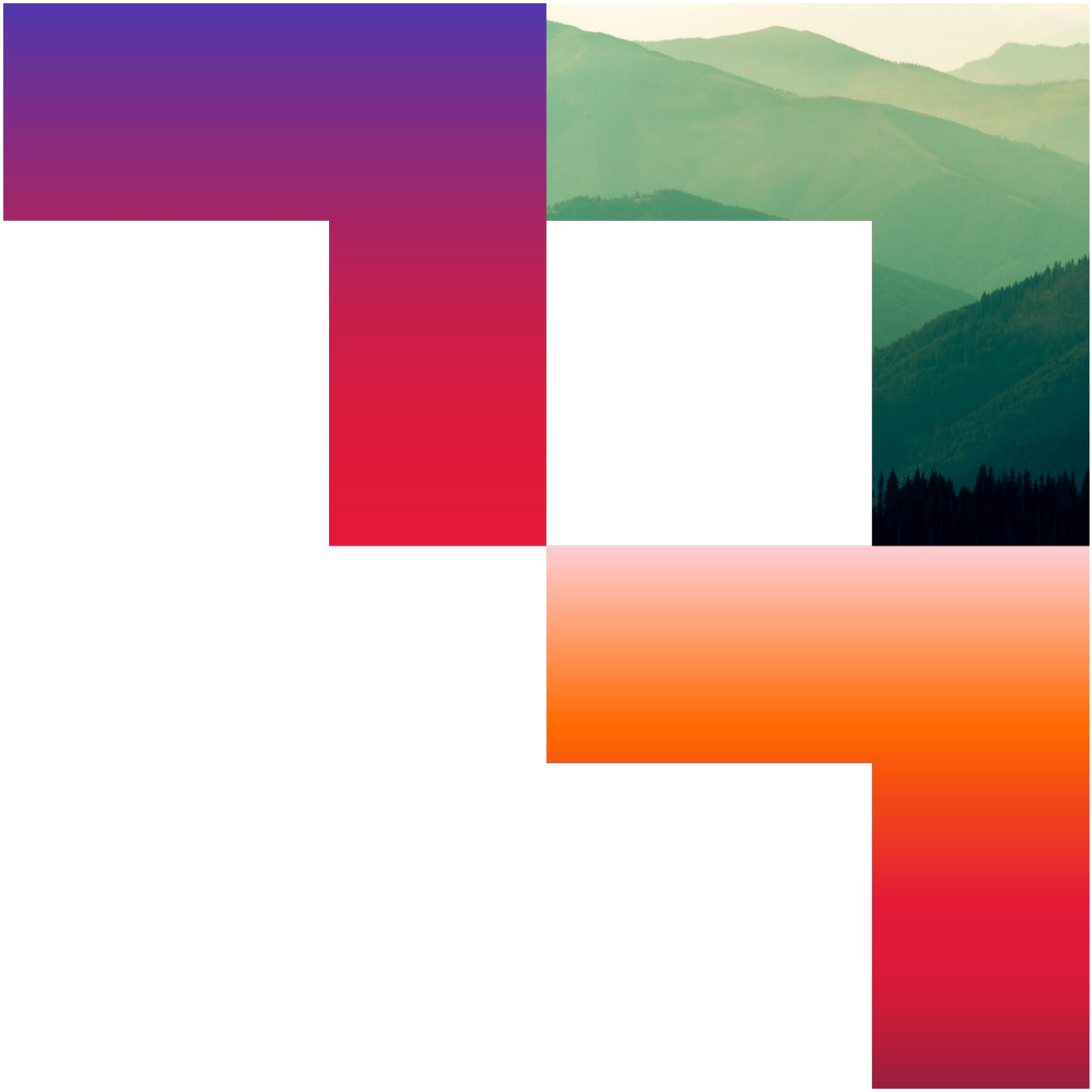


Private Cloud Hosting Service

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

Table of contents

1. Service Description 4

1.1. Features and Options 4

1.2. Service Delivery and Approach 5

1.3. Community Cloud 6

1.4. Compliance 8

1.5. OFFICIAL Vulnerability Management and Protective Monitoring 9

1.6. OFFICIAL Data Management and Handling 13

1.7. Management of Virtual and Dedicated Resource Pools 13

1.8. Capacity Management, Expansion and Reporting 15

1.9. Resilience 16

2. Data backup and restore. 18

3. Service Continuity 18

4. Onboarding and Offboarding 19

4.1. Onboarding 19

4.2. Offboarding 19

4.3. Cloud Security Principles 20

5. Service constraints. 26

6. Service Levels 26

6.2. Service Management 28

7. After sales support 28

8. Technical requirements 29

9. Outage and maintenance management 29

9.1. Event Management 29

9.2. Scheduled Maintenance 29

10. Hosting options and locations 29

11. Security 29

12. Service Pricing and Terms and Conditions 30

12.1. Pricing 30

12.2. Terms and Conditions 30

13. Further information 30

PROPRIETARY AND CONFIDENTIAL 31

© 2026 CGI IT UK Ltd

Service Definition overview.

CGI is primed to deliver specialised Private Cloud solutions, custom-built for UK government organisations and agencies, leveraging our extensive decades-long expertise in the industry. Our unwavering commitment is to uphold the highest standards of security, compliance, and data protection, while aligning seamlessly with stringent government requirements.

We deliver complicated management, integration services and solutions leveraging, industry leading marketplace technologies, to help resolve today's IT challenges such as transforming away from legacy applications, eliminating technical debt, and reducing operational costs.

CGI dynamically brings you best-of-breed Private Cloud services and solutions, to not only help you deliver today’s business outcomes, but also be ready for tomorrow's IT challenges. Leveraging our extensive decades-long expertise in the industry, our unwavering commitment is to uphold the highest standards of security, compliance, and data protection, while aligning seamlessly with stringent government requirements.

Our current government clients frequently attest to the fact that our cloud hosting solutions meet the highest standards of compliance, and performance while enabling agility and scalability to effectively deliver and meet their requirements.

Why CGI?

With a firm focus on delivering optimal value for money, we combine our deep industry experience and partner network with innovative technology to provide trusted, cost effective Private and Public Cloud management support and innovative solutions to help you deliver your critical business applications and user services.

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. We are insights-driven and outcomes-based to help accelerate returns on our client's IT investment. Across 21 industry sectors in 400 locations worldwide, our 91,500 professionals provide comprehensive, scalable, and sustainable IT and business consulting services that are informed globally and delivered locally.



Figure 1 - CGI's Ecosystem of Technology Partners

In addition to our Private Cloud support offerings, we excel in seamlessly integrating your on-premise systems with public cloud IaaS and PaaS services. This expertise enables us to create dynamic hybrid cloud solutions tailored to meet your specific hosting and application delivery needs. Embracing the best of both public and private cloud technologies, our hybrid cloud approach ensures flexibility and scalability while accommodating even the most specialised client requirements.

Partner Ecosystem

Google and with over 150 technology companies including Dell, VMWare, Oracle, RedHat, NetApp, Microsoft, Google and Amazon, so that we can bring you best-of-breed Private Cloud and hybrid cloud services and solutions leveraging, industry leading marketplace technologies, to not only help you deliver today’s business outcomes, but also be ready for tomorrow's IT challenges such as transforming away from legacy applications and eliminating technical debt and removing obsolescence.

© 2026 CGI IT UK Ltd

1. Service Description

1.1. Features and Options

CGI's services have been designed to support the government ICT strategy and the Digital by Default Service Standard. This includes a focus on:

- Understand the user (and client) needs, underpinned by CGI's multi cloud strategy and an emphasis on ensuring our clients use the right cloud for the right workload at the right time.
- Implementing the National Cyber Security Centre (NCSC) 14 cloud security principles and 10 steps to Cyber Security.
- Reducing waste and project failure and stimulating economic growth.
- Using ICT to enable and deliver change.
- Strengthening governance.
- Using the ITIL Framework for IT Service Management.
- Supporting agile and providing a flexible service to our clients.
- Support open standards.
- Provide transparent reporting on service availability and reporting, ensuring the baseline service is fit for purpose.

1.1.1. Green IT

CGI's IaaS services support the governments Greening ICT Strategies. CGI recognises that its operations can impact both directly and indirectly on the environment. Our goal is to protect the environment through good management and by adopting best practice throughout our organisation. We work to integrate environmental considerations into our business decisions, consultancy, and client solutions. Indeed, the Equinix data centre where we host our most recently provisioned node won the Green Data Centre award from data centre Dynamics, and this innovative use of sustainable and renewable energy technology was a key factor in us selecting the facility for our operations.

1.1.2. Infrastructure as a Service (IaaS)

Our CGI Private Cloud has been built to meet demand for cloud infrastructure that provides high security, enterprise-ready features, and the ability to support mission and business critical workloads.

Private Cloud supports complex and rapidly evolving requirements, such as giving you the ability to deploy thousands of servers in minutes, scale to test services and meet demand, and automate software development and deployment processes.

The service supports UNCLASSIFIED, OFFICIAL and OFFICIAL SENSITIVE marked data workloads, offers a choice of both virtual and bare-metal infrastructure and various billing options.

1.1.3. Multi-Cloud Approach

As part of this service clients are able to leverage CGI's partnerships with the leading hyper scale public cloud providers and utilise the services offered by these providers. This includes:

- CGI Private Cloud (this offering)
- Additionally:
  - CGI Cloud Connect
  - Amazon Web Services (AWS) – PSN Accredited and Commercial
  - Google Cloud Platform

Oracle Cloud Infrastructure:

- Microsoft Azure – Government and Commercial.

© 2026 CGI IT UK Ltd

1.1.4. Data Centres

Our Private Cloud data centres meet the Uptime Institute Tier 3 requirements, which includes the following specifications:

- Multiple independent distribution paths serving IT equipment. Generally, only one distribution path serves equipment at any given time.
- All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

1.1.5. Network and PSN Connectivity

Our services utilise an assured data transport mechanism. CGI can provide PSN Protect network connectivity. We can also provide VPN over internet where required.

1.2. Service Delivery and Approach

1.2.1. Infrastructure Service Portfolio

CGI Infrastructure Services portfolio provides a range of scalable hybrid cloud platforms. Incorporating Enterprise, Public Sector and Public cloud services, CGI's broad portfolio can support the client's business's cloud requirements offering scalability, security, and a range of support services.

	Enterprise Cloud	Private Cloud	Public Cloud
IaaS - Services	Designed for commercial mid-market and Enterprise organisations requiring geo-diversity and private connectivity. Delivers highly available application uptime for critical business applications.	Designed for the Public Sector, including local authorities. Capable of delivering services to organisations connected via the Public Services Network (PSN). Up to OFFICIAL classification, including OFFICIAL SENSITIVE handling.	Designed to support organisations with highly fluctuating requirements and global installation requirements across availability zones.

Table 1 Infrastructure Services Portfolio

With our UK-based data centres, CGI provides gate-to-rack control of our UK-based Enterprise cloud platform. For our Private Public Sector cloud platform, CGI leverages the highly secure UK Public Sector approved data centres provided by ARK. Using these sites provides guaranteed data sovereignty, ensuring that the client's data will never be hosted outside of UK borders. ISO 27001 and PCI certified data centres provide additional peace of mind. Clients with services resident within Crown Hosting Services will also benefit from low latency interconnections due to the immediate physical proximity of the CGI Public Sector Cloud to Crown Hosting Services.

Integration with Next Generation Network enables us to provide high-speed, uncontended connectivity across all cloud platforms and L3VPN connectivity to client sites. Delivered as a fully managed enterprise-grade, low-latency service, CGI managed connectivity services can form the building blocks of the client's network infrastructure.

CGI is able to leverage ExpressRoute and Direct Connect to integrate public cloud connectivity directly into our network and cloud solutions, enabling the client to build and deploy hybrid cloud solutions across the CGI Enterprise Cloud platform and public cloud providers.

1.2.2. CGI Private Cloud Architecture

CGI Private Cloud for the Public Sector has been designed to provide a highly available, highly scalable Infrastructure as a Service (IaaS) platform for client solutions.

Based on tier 1 Enterprise-grade hardware, the platform includes the following:

- Options for virtual or physical servers.
- Options for resource pools or named servers.

© 2026 CGI IT UK Ltd

- CGI Secure Hybrid Cloud Management Platform.
- Geo diverse data centres.
- Options for Managed or Unmanaged Virtual Firewalls.
- Options for Managed or Unmanaged Virtual Load Balancers.
- Internet and L3VPN (MPLS) connectivity.

Our platform is deployed in 2 availability zones across separate DCs, including multiple application tiers, managed virtual load balancer, managed virtual firewalls and a 3rd party Global Load Balancing solution.

1.2.3. Platform Options

Within the Cloud Platform, clients can choose between a Community Cloud Service or a Dedicated Private Cloud Service:

	Private Cloud	
	Community Cloud	Dedicated Cloud
What you get	Shared hardware with options for physical servers – proven best practice architecture, built and managed by CGI	Hardware dedicated to the client – designed to a CGI proven architecture, built, and managed by CGI
How it is managed	CGI Secure Hybrid Cloud Management Platform	CGI Secure Hybrid Cloud Management Platform
Why you would choose this	Platform built and managed locally in the UK from ARK Data Centres providing local accountability and control. Flexibility of design and capability beyond public cloud Predictable costs	Security or performance conscious. Not wishing to share resources with other clients. Specific compliance requirements
What you need to consider	Cannot use existing Windows Server licences. Need Software Assurance on existing licences for mobility. Ceiling limits on some resources	The platform has to be specified to cater for all fluctuations of use; does not benefit from consume on demand capability. OPEX and no hardware EoL. The client can utilise their existing licensing without requiring Software Assurance Leverages a proven design and expert resource to build and manage
Availability/Pricing	Standard product and pricing including PAYG model, available immediately	Built on demand to the client requirement

Table 2 - Cloud Deployment Options

1.3. Community Cloud

1.3.1. Network

Within the clients' Public Sector Cloud solution, CGI will provide a number of core network components that will include the following:

© 2026 CGI IT UK Ltd

- Virtual Server Network Card – Up to four network cards per virtual server which can be connected to any VLAN's within the client's environment.
- VLAN – Up to 100 VLAN's per client solution for use as LAN or DMZ networks.
- Internal IP Addressing – A /24 private IP address range will be assigned to each VLAN be default, optionally this can be extended up to a /21 private IP range upon request.
- Public IP Addresses – /29 (3 useable), /28 (11 useable) or /27 (27 useable) blocks of useable public IP addresses.
- Public DNS Services – CGI will provide access to our public facing DNS service for Internet name resolution.
- Managed Virtual Firewall – A range of Managed Virtual Firewalls are available including a selection of bandwidth, add-on services and high availability.
- Managed Virtual Load Balancer – An optional element is a range of virtual load balancers.
- Internet Breakout –resilient Internet breakout, additional bandwidth can be purchased on request.
- L3VPN Connectivity – Resilient or non-resilient connectivity to a CGI L3VPN service.
- DDoS mitigation service protecting against flood type attacks (e.g. DNS amplification and SMURF attacks) for all external IP addresses.

1.3.2. Virtual Server Network Card

Within each virtual server, CGI supports up to four virtual network cards. Each virtual server can be connected to any VLAN available within the client solution. The virtual network cards can be configured as E1000 (1GiBps) or VMXNET 3 (10GiBps) adapters. Within a virtual resource pool, all network cards are connected to client specific VLAN's on a shared distributed virtual switch.

1.3.3. VLAN

VLAN's are configured within a client VRF providing logical per client isolation. VLAN's are per cloud platform. During the initial deployment CGI will deploy VLAN's in line with the agreed solution design, clients can configure additional VLAN's as required through the vCloud Director Web interface or API.

Within the Public Sector Cloud platform site, any VLANs created will be available to the virtual platform as well as any dedicated physical or other platform services, such as OVM, that CGI might provide. CGI does not support stretched VLAN's between data centres.

1.3.4. Internal Private IP Addressing

For each VLAN provisioned, CGI will allocate a /24 private IP address range, if this range conflicts with an existing IP address range within the client's network, the client can request that is it changed prior to the configuration of any virtual machines for no additional cost.

Once virtual machine and firewall configuration has been completed, changing the private IP address range will be charged at standard professional services rates.

1.3.5. Public IP Addresses

Non-transferable Public IP addresses blocks are provided by CGI.

IP address availability will be subject to the network design defined in your low-level design. The minimum number of useable addresses will be as follows:

- /29 – 3 useable public IP addresses
- /28 – 11 useable public IP addresses
- /27 – 27 useable public IP addresses.

Larger Public IP Address blocks may be available upon request.

1.3.6. Public DNS Service – Internet Name Resolution

CGI will provide two public facing DNS service IP addresses. The service is built on a resilient multi-site infrastructure ensuring continuous availability.

© 2026 CGI IT UK Ltd

1.3.7. Virtual Firewall

As part of the Public Sector Cloud solution, CGI will provision a virtual firewall solution. A range of options are available for the virtual firewall solution including both unmanaged and managed solutions.

1.3.8. Perimeter Firewall

As part of the Public Sector Cloud infrastructure CGI deploy and manage a perimeter firewall for all clients, this appliance provides a second layer of firewall protection in addition to any firewall solution the client deploys.

1.3.9. Virtual Load Balancer

Within the Public Sector Cloud Platform, CGI provides the option of a dedicated virtual load balancer. A range of options are available for the virtual load balancer including both unmanaged and managed solutions.

1.3.10. Internet Breakout

As standard, if the client has purchased Internet breakout, CGI will provide a resilient Internet service. This service is an unfiltered Internet service delivered through the Public Sector Cloud resilient network fabric.

If additional bandwidth, Internet Protection (such as DDOS) or security services are provided, these are available as optional add-on products.

1.3.11. Managed WAN

The Public Sector Cloud platform fully supports the delivery of CGI L3VPN connectivity directly into the platform providing connectivity to existing client sites.

L3VPN connectivity will be terminated on the 10GiBps Public Sector Cloud network fabric and delivered over the resilient network connectivity to the client cloud network.

If the client has an existing 3rd party MPLS, CGI can integrate with it by utilising a cross connect at any one of our nationwide POP's. From there, CGI will use our Next Generation Network to deliver the client's services as a L3VPN to the Public Sector Cloud platform.

Please note there may be additional charges from the client's MPLS provider to cross connect with CGI.

1.3.12. DDoS Mitigation

All ingress internet traffic to the public-sector cloud is subjected to volumetric (L3/L4) DDOS mitigation protection. This is achieved by passing all traffic via a UK primary scrubbing centre, with 4 TBps of attack ingestion capacity, before delivering clean traffic, using BGP routing, to the **6DG public sector cloud.** DDOS protection is always on capturing attacks at the moment they occur, using advanced behaviour analytic technology and reactive IP filtering through null routes and limited ACL filtering.

1.4. Compliance

Where CGI is providing Services that are Compliant with a Specified Standard, you should be aware that only the Services we are providing carry an accreditation. Anything you use those services for does not inherit the accreditation from the Services on which it sits.

1.4.1. OFFICIAL Data Security Policy

CGI is an accredited company under ISO/IEC 27001:2013 and OFFICIAL / OFFICIAL SENSITIVE and, as such, adheres to the approved security policy noted below.

It is the policy of the organisation to ensure that at CGI:

- Information will be protected against unauthorised access.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Regulatory and legislative requirements will be met.
- Business continuity plans will be produced, maintained, and tested.
- Information security training will be available to all staff.

© 2026 CGI IT UK Ltd

- All breaches of Information Security, actual or suspected, will be reported to and investigated by the Information Security Manager.

1.4.2. Official Information Assurance

It is the policy of the company to protect all information against unauthorised access while maintaining the confidentiality and integrity of that information. We comply with all regulatory and legislative requirements and maintain and test a comprehensive business continuity plan.

1.4.3. Data Processing

CGI is registered as a data controller under the Data Protection Act 2018 and has a Data Protection Officer to oversee the specific administrative implications of this particular Act who can be contacted regarding any Data Protection issues.

1.4.4. OFFICIAL Hard Disk Destruction

Any assets, which have been assessed and classed as defective, end-of-life or no longer fit for purpose will be securely destroyed in a way that makes reconstitution unlikely in accordance with:

- HMG Information Assurance Standard Number 5 (IAS5) – Secure Sanitisation.
- CPNI Standard 2013062 – Secure Destruction of Sensitive Items.
- NCSC Secure Sanitisation of Storage Media.

1.4.5. PCI-DSS

CGI ensure all its certified PCI-DSS Services are maintained according to the relevant PCI-DSS requirements to ensure the security of cardholder data on behalf of the Client. This ONLY applies to Services which CGI provides. The Client must ensure that all its own functions relating to cardholder data, application or otherwise, are both PCI-DSS certified and maintained, and that all relevant steps are taken to protect cardholder data.

1.5. OFFICIAL Vulnerability Management and Protective Monitoring

Regular IT Health Checks will be conducted to ensure CGI systems remain patched. To provide interim views of vulnerabilities, CGI can provide a proactive Qualys scanning service, which alerts on any unpatched or at-risk services.

CGI adheres to the following Event Management Logs for its OFFICIAL management platform.

Record events affecting the system:

- Activity logs.
- Transaction logs.
- Authentication events (success, failure).
- Credential changes or resets.
- Hardware and software events (including failures).
- Privilege changes for users.
- Tie individual users to their actions in order to make them accountable.

Record events such that the record is:

- Evidential (to a suitable standard for the system).
- Tamper evident or tamperproof..

Process EVENTS to reveal INCIDENTS:

- Raise alerts automatically.

CGI's Event Logs follow the Protective Monitoring Controls (PMCs) in accordance with NCSC's Good Practice Guide 13 (GPG13) documentation against attacks made via the various Compromise Methods defined in our security assurance documentation. CGI focus our attention to ensure the following logs are monitored on a daily basis and reviewed by a senior member.

© 2026 CGI IT UK Ltd

- PMC1 Accurate time in logs.
- PMC2 Recording of business traffic crossing a boundary.
- PMC3 Recording relating to suspicious activity at the boundary.
- PMC4 Recording of internal workstation, server, or device status.
- PMC5 Recording relating to suspicious internal network activity.
- PMC6 Recording relating to network connections.
- PMC7 Recording of session activity by user and workstation.
- PMC8 Recording of data backup status.
- PMC9 Alerting critical events.
- PMC10 Reporting on the status of the audit system.
- PMC11 Production of sanitised and statistical management reports
- PMC12 Providing a legal framework for Protective Monitoring activities.

The configuration and associated processes of CGI OFFICIAL management platform relate to the highest levels of implementation guidance for NCSC's 14 Cloud Security Principles:

1. Data in transit protection
2. Asset protection and resilience
3. Separation between consumers
4. Governance framework
5. Operational security
6. Personnel security
7. Secure development
8. Supply chain security
9. Secure consumer management
10. Identity and authentication
11. External interface protection
12. Secure service administration
13. Audit information provision to consumers
14. Secure use of the service by the consumer.

In addition, CGI build and manage cloud environments in accordance with NCSC's 10 steps to Cyber Security:

1. Risk management
2. Engagement and training
3. Asset management
4. Architecture and configuration
5. Vulnerability management
6. Identity and access management
7. Data security
8. Logging and monitoring
9. Incident management
10. Supply chain security.

1.5.1. Consumption Model

The Client may consume Public Sector Cloud resource in two models. Each platform solution is restricted to a consistent model.

- Resource Pools – A resource pool provides the client with a pool of vCPU, RAM, and storage with the capability to create, remove or resize virtual servers as required.

© 2026 CGI IT UK Ltd

- Named Servers – Named Servers are pre-defined virtual or physical servers with a defined resource configuration for the term of the contract, if the client wishes to modify the resource specification of the server this would be treated as a change order.

The client can choose to purchase a resource pool with shared resource, or the client can choose to have dedicated resource, meaning that vCPU and RAM will be provided from dedicated hardware.

The client specifies the amount of resource they require in terms of vCPU, vRAM and Storage. Then, through CGI Secure Hybrid Cloud Management Platform, CGI will manage the deployment and provision of servers and associated resources. The client can change resource specifications and servers as often as they like within the confines of the resource pool they have purchased.

1.5.2. Resource Pool - Virtual

The options available for a virtual resource pool are as follows:

- vCPU– 1 TO 1500
- vRAM 1 TO 3500TiB
- SAN Storage – 100GiB to 100TiB.

Within a virtual resource pool, the compute resource is provided from a pool of multi-tenant compute nodes. These nodes are configured as a single shared compute cluster with N+1 high availability at a platform level.

Within a virtual resource pool, there are a predefined maximum per virtual server configuration rules in place. These include:

- vCPU –Maximum of 24 vCPU per virtual server
- vRAM – Maximum of 256GiB RAM per virtual server
- Storage – Maximum volume size of 2TiB with no more than 10TiB per Virtual Server.

1.5.3. Resource Pool - Dedicated

The options available for a dedicated resource pool are as follows:

vCPU	vRAM	Storage	Physical Compute Node	Expansion Increment
224	115	100GiB to 100TiB	Dual Intel Xeon Scalable, 128GiB RAM	Per 115GB RAM
224	230	100GiB to 100TiB	Dual Intel Xeon Scalable, 256GiB RAM	Per 230GB RAM
224	465	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
448	930	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
672	1,395	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
896	1,860	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
1,120	2,325	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
1,344	2,790	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM
1,568	3,255	100GiB to 100TiB	Dual Intel Xeon Scalable, 512GiB RAM	Per 465GB RAM

Table 3 Resource Pool: Dedicated

Within a dedicated resource pool, the underlying compute hardware is dedicated to the client, CGI recommend a maximum over subscription ratio of 4:1, however, the client may choose to exceed this amount if their workload is appropriate.

The underlying compute hardware will be configured in an N+1 configuration providing high availability in the event of a compute node failure; the useable vRAM purchased takes into account the high availability configuration.

CGI recommends a minimum of 100GiB of storage is allocated for system drives on all virtual servers.

© 2026 CGI IT UK Ltd

For clients with a dedicated resource pool, there must be 10% space free on all data stores to enable the platform-level snapshots to complete successfully. If the free space falls below this amount, the daily platform level snapshots will not be available.

Within a dedicated resource pool there are a predefined maximum per virtual server configuration rules in place, these include:

- vCPU –No limit.
- vRAM – Limited by the per compute node physical RAM, recommendation that no virtual machine exceeds 25% of the underlying per compute node RAM as listed in the specification table above.
- Storage – Maximum volume size of 2TiB with no more than 10TiB per Virtual Server.

1.5.4. Oracle SPARC

Oracle SPARC is only available per physical server based on a minimum 12-month commitment. As standard each physical server is an Oracle T7 server with 32 cores (224 vCPU) and 488GB RAM. Other configurations are available on request.

1.5.5. Management of Resource Pools

Virtual and Dedicated resource pools will be managed by CGI using our Secure Hybrid Cloud Management Platform.

1.5.6. Named Servers

By purchasing named servers, the client does not have to purchase a pool of resource that may not be fully utilised. The client gets to choose between virtual servers and physical servers.

The following specifications are available:

VIRTUAL SERVERS	PHYSICAL SERVERS
vCPU – 1 to 24	CPU – Choice of 2*4 Core 2.6GHz 2*10 Core 2.4GHz 2*14 Core 2.6GHz 2*18 Core 2.7GHz.
vRAM – 1 to 256GiB *RAM deployed as fixed – not contended	RAM – 64, 128, 256, 384, 512, 768GiB
System Drive – 100GiB to 500GiB Available in 100GB increments	Local Drive - Choice of 2x600GiB 15K SAS RAID 1 2x480GiB SSD RAID 1 6x600GiB 15K SAS RAID 6 6x480GiB SSD RAID 6.
Storage Drive – 100GiB to 2TiB Up to five storage drives per Virtual Server Available in 100GiB increments	Shared SAN storage may also be provided for physical servers

Table 4 Named Servers

All virtual servers are fully licensed for any current edition of Microsoft Windows Server; for Physical Servers, the appropriate licensing must be specified and purchased.

© 2026 CGI IT UK Ltd

1.5.7. Storage and Storage presentation

The Public Sector Cloud Platform utilises Solid State Drives (SSD) to deliver a high performance, highly resilient storage architecture. All storage is provided from Enterprise grade SANs with integrated resiliency, Redundant Array of Inexpensive Disks (RAID), hot spare drives and storage encryption at rest.

Storage is presented to virtual machines as a VMDK within the Virtual Cloud Platform.

1.5.8. Bandwidth and Throughput.

Server performance is highly affected by storage throughput Read/Write speeds. These can vary during the day and throughout each month on the platform due to usage patterns. Please note that different applications can utilise storage in different ways: the default file sizes that they read and write, and how reading/writing is processed with single or multiple threads. Both can affect the performance the client may see for typical transfer speeds.

The storage platform is designed to provide 2 IOPs per GiB storage per logical disk.

1.6. OFFICIAL Data Management and Handling

1.6.1. Data Migration

CGI can and will return all client generated data as agreed in a relevant call-off agreement. Once data has been returned and confirmed by the client and, if asked to do so, CGI will purge and destroy all data belonging to the client or consumer from any computers, storage devices and storage media that are to be retained after the end of the subscription period and the subsequent extraction of consumer data.

1.6.2. Data Storage and Processing locations

Our IaaS services are delivered for the Public Sector Cloud platform from four locales; these sites are physically and geographically separate, with no interdependencies. Data is unable to pass from one locale to another (excluding replication for disaster recovery purposes) without being deliberately migrated as a result of a client decision to do so.

1.6.3. OFFICIAL Data Handling

CGI and their suppliers adhere to the HMG Security Policy Framework (SPF) and Government Functional Standard GovS 007: Security for information handling requirements. (The Government Functional Standard replaces the Security Policy Framework. The policies which sit within that framework remain in effect but are now in support of this standard).

CGI Public Sector Cloud documentation will be marked in accordance with our internal data classification policy (and under the Government Security Classification Policy (GSCP) is likely to be considered OFFICIAL Sensitive at most) with stringent need to know controls applied.

Documents relating to the IaaS environment, its design and operation are stored securely within electronic storage repositories with strict access control policies in place.

Processes employed for secure erasure of media will be detailed in CGI Public Sector Cloud Security Operations Procedures (SyOPs) documentation developed by the appropriate service provider. These must conform to CGI standing documentation, HMG policy and IAS5.

1.7. Management of Virtual and Dedicated Resource Pools

1.7.1. CGI Secure Hybrid Cloud Management Platform (SHCMP)

The Cyber Essentials Plus certified CGI Secure Hybrid Cloud Management Platform (SHCMP) provisions software-defined data centre services as virtual data centres that provide virtualised compute, networking, storage, and security. This platform allows CGI to create templates with single or many virtual servers with associated configurations, build, networking, and storage components. CGI can quickly and easily manage complex cloud deployments, effect change, apply patches through automation whilst also delivering remote management and monitoring of all servers across multiple hypervisors. The CGI Secure Hybrid Management

© 2026 CGI IT UK Ltd

Platform is an over-arching toolset that allows CGI to securely deliver management capabilities up to and including OFFICIAL SENSITIVE to multiple cloud environments from different cloud providers in many locations from a single management platform.

This platform delivers the following capabilities:

- Monitoring and Management of Server instances and storage.
- Orchestration of Server instances, Storage allocations and network provision within the hypervisors.
- Patch Management.
- Antivirus.
- Automation.
- Templating of individual and multiple server, storage, and network configurations for fast, repeatable deployments.

For services purchased as virtual or dedicated resource pools, CGI will provision the resource pool, network components and virtual firewall in accordance with our default configuration.

Optionally, CGI can provision individual Virtual Servers to a defined base template. The client must specify the quantity of virtual servers required along with CPU, RAM, storage partitioning, network information and the operating system selection. CGI will deploy a template virtual server to the defined specification and update the server with the latest available security and critical updates.

1.7.2. Management of Named Virtual Servers and Physical Servers

For solutions with named virtual servers or physical servers, by default all network components and virtual servers are provisioned up to the operating system install.

Servers will be deployed within a workgroup unless additional professional services have been purchased for migration or further implementation work.

1.7.3. Managed Antivirus

CGI delivers a managed antivirus service as part of the standard configuration on all Virtual Hosts, Virtual Machines and Physical Machines.

1.7.4. Licensing

As part of the CGI Public Sector Cloud platform, there are multiple licensing options available. These include:

- Microsoft SPLA – CGI can provide Microsoft licences for SQL and Applications on a monthly basis; these licences are rented and can be used within the CGI Public Sector Cloud platform or on-premises where the servers are under CGI administrative control. Clients utilising this licensing model have included software assurance to always be able to use the latest version of the software, it also includes downgrade rights enabling the use of previous versions of Microsoft products.
- Microsoft CSP – CGI is a Microsoft Cloud Solution Provider (CSP), this status enables us to provide Office 365 based licensing for use within our Public Sector Cloud platform, as well as Public Cloud services on Azure and Office 365.
- Open/Select/EA – If a client has an existing volume licence agreement, certain licences can be used within the CGI Public Sector Cloud as long as they have active Software Assurance, exceptions include Windows Server and Microsoft Office licences. In the event that a client wishes to utilise their existing licensing, they must complete a Licence Verification Mobility form and submit this to their Microsoft representative or reseller.

NOTE: It is the client's responsibility to ensure they are appropriately licensed for all software used within the CGI Public Sector Cloud platform above the Operating System.

1.7.5. Supported Operating Systems

All solutions are fully licensed for any currently supported release of Microsoft Windows Server; however, other operating systems are available, including Red Hat Enterprise Linux.

It is the client's responsibility to ensure that the appropriate licensing and support has been purchased for any virtual servers running on the CGI Enterprise Cloud platform.

© 2026 CGI IT UK Ltd

Supported Operating Systems include the following:

Microsoft Windows	Linux
Microsoft Windows Server 2019	Suse Linux Enterprise 12
Microsoft Windows Server 2022	Suse Linux Enterprise 15
	Red Hat Enterprise Linux 7
	Red Hat Enterprise Linux 8
	Red Hat Enterprise Linux 9
	Ubuntu 22.04 Server
	Ubuntu 24.04 Server

Table 5 - Supported Operating Systems

Support options for older operating system versions with active Extended Life Support or Extended Security Update Support in place are available as an additional service.

1.7.6. Consumption-based Licensing

Where the client is using a consumption-based billing model for the Public Sector Cloud platform, it is important to note that although the platform is fully licensed for Windows Server, any other chargeable licences have a minimum term of one (1) month. In the event that a virtual server is started using a chargeable licence, the client will be charged for a minimum of one (1) months' worth of licence usage.

1.8. Capacity Management, Expansion and Reporting

1.8.1. Resource Pool – Virtual

To manage resource consumed within the resource pool; the client must order additional resource in advance of being required through a change request or the request for service (RFS) process.

Total resource available will be as invoiced and resource consumed will be the sum of the provisioned machines.

CGI operates an industry standard ratio of 4:1 for virtual to physical core allocation.

1.8.2. Resource Pool – Dedicated

It is the client's responsibility to manage resource consumed within the resource pool; the client must order additional resource in advance of being required.

Additional resource can be added in fixed quantities. Total resource available will be as invoiced. Resource consumed will be the sum of the provisioned machines.

1.8.3. Named Virtual Servers

It is the client's responsibility to manage resource consumed within a named virtual server.

Virtual Servers can be expanded via a sales order. Physical server RAM and storage can be upgraded in line with the defined physical server models available. Physical server CPUs are fixed after the initial purchase.

1.8.4. Logging

CGI will maintain the following logs for our Public Sector Cloud platform:

Item	Type	LIVE	Archive
Network Fabric	Critical and Warning	1 Year	2 Years
Storage Fabric	Critical and Warning	1 Year	2 Years
Storage Array	Critical and Warning	1 Year	2 Years

© 2026 CGI IT UK Ltd

Item	Type	LIVE	Archive
Compute Hardware	Critical and Warning	1 Year	2 Years
VMWare ESXi Host	Critical and Warning	1 Year	2 Years
Oracle VM for X86	Critical and Warning	1 Year	2 Years
Oracle SPARC	Critical and Warning	1 Year	2 Years

Table 6 - Public Sector Cloud Logging

Current logs are immediately available; archive logs are available on request and will be provided within 48 hours.

1.8.5. Platform Patching

As part of providing the Public Sector Cloud platform, CGI provide ongoing maintenance and management of the underlying hardware supporting that platform. Patching of the platform will be carried out in line with our platform patching policy.

All patching is carried out using the following process:

- Scan of the device to identify missing Critical and Security patches.
- All patches identified are tested within our lab environment prior to production deployment.
- Request for Change (RFC) raised internally to approve patch installation during a pre-agreed maintenance window.
- Patches installed during the maintenance window.

The only exception to the above will be in the event of a known critical or Zero-day exploit. In the event of a critical exploit being identified which is prevalent in the wild, CGI reserves the right to carry out emergency maintenance on the platform to address the exploit.

1.8.6. Data Migration and Implementation

CGI has a wide range of migration, implementation, and other professional services available beyond the standard Public Sector Cloud build. These services integrate closely with our Public Sector Cloud platform to provide a seamless client experience from the provision of virtual machines to the migration of data or services into the Public Sector Cloud Platform. If you're interested in these services, please contact your Account Manager.

1.8.7. Bespoke Solutions

If the solution the client requires is not covered by the specifications provided within this document, CGI can provide a wide range of bespoke solutions utilising our knowledge of industry best practice design to deliver a custom Public Sector Cloud platform that meets the client's specific requirements.

For any custom solution, CGI will work closely with the client to build a clear detailed specification and to agree the statement of work and deliverables ensuring that the solution delivered meets the client expectations.

1.9. Resilience

Our systems are designed to be highly reliable and available, but we recognise that is not always enough to ensure continuous delivery of key services and as a result provide a full range of business continuity and backup services.

1.9.1. Backup and Restore

Backup services are provided using industry leading technologies for both agentless snapshot and agent-based offering.

1.9.2. Supported Configurations

Backups are configured in line with client data retention and back up frequency requirements.

© 2026 CGI IT UK Ltd

1.9.3. Service Summary

The following table provides a summary of the service provided under this Service Description:

Service Area	Service Feature
Backup	Backup policies
	Data storage
Restore	File level restore
	Server level restore

Table 7 - Back Up and Restore Service Summary

1.9.4. Detailed Service Description

Service Feature	Description	Client obligations	Limitations
Backup			
Backup policies	Backup policies will be setup as per the client requirement on a per server basis	The client is responsible for defining their backup frequency and length of data storage requirements.	
Data storage	Storage will be provisioned to store data as defined by the client's backup policy. Backup data storage is charged on a per GB basis. Data is stored on site but off SAN, with the option of offsite storage.	The client is responsible for defining their backup architecture. Charges will apply at the published rate for all storage used and for node-to-node data transfer if applicable.	
Restore			
File level restore	Specific files and or folders may be retrieved on written request from the client.		Clients are limited to 4 restores per server per year. Additional restores available on a per incident basis.
Server level restore	A complete server image will be restored to the state of the last successful backup upon client request	Clients will be required to verify the server before it is migrated into the production environment to replace the original server image.	Clients are limited to 4 restores per server per year. Additional restores available on a per incident basis.

Table 8 - Back Up and Restore Service Description

1.9.5. Disaster Recovery

Our services can be mirrored across multiple infrastructure nodes in the UK. Multiple nodes can be used to support disaster recovery objectives as well as tactical and business continuity requirements.

1.9.6. Multi-site mirroring

Multi-site resilience is enabled by providing resources in more than one cloud node.

© 2026 CGI IT UK Ltd

1.9.7. Supported Configurations

Supported configurations range from the ability to restore from backups to non-reserved resources in a second node to active-active multi-node operation.

1.9.8. Service Summary

The following table provides a summary of the service provided under this Service Description:

Service Area	Service Feature
Disaster Recovery	Server level restore
	Active slave
	Multi-site network

Table 9 - Multi-site mirroring Service Summary

1.9.9. Detailed Service Description

Service Feature	Description	Client obligations	Limitations
Disaster Recovery			
Server level restore	The complete server images for a solution will be restored to the state of the last successful backup in an alternative cloud node upon client request.	Clients will have to decide if they are to restore to reserved instances or un-reserved instances when selecting this service feature.	Un-reserved instances are not guaranteed to be available. Reserved instances are guaranteed to be available
Active slave	Permanent committed resources will be made available to support multi-site slave configurations at the platform or application layer.	Clients will have to specify the parameters within which the active slave system needs to operate.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.
Multi-site network	Networking available in multiple cloud nodes to support DR and BC requirements.	Clients will need to decide if they are to opt for reserved or committed network resources.	Should low latency be critical for application performance this service can only be guaranteed to be performant with testing.

Table 10 - Service Description

2. Data backup and restore.

Our comprehensive approach includes using best of breed technologies to implement and enforce data availability and data consistency features such virtual machine (VM) image and data replication across, alternative regional hosting locations, application failover mechanisms, robust backup and restore regimes, in conjunction with meticulous disaster recovery planning.

3. Service Continuity

Empowering government services to operate without interruption, our hosting solutions are designed to provide resilient disaster recovery and business continuity features. In the face of unforeseen incidents or disasters, we can help to ensure uninterrupted service availability and seamless data accessibility.

© 2026 CGI IT UK Ltd

At every step, we collaborate closely with you, starting from the requirements specification stage. Our goal is to craft a solution that not only addresses your daily service availability needs but also aligns with your Recovery Time Objective (RTO), Recovery Point Objective (RPO), and data retention and security governance. By meticulously designing each aspect of the solution together, we ensure it's not just a fit for your present demands but also future-proofed for scalability and resilience.

4. Onboarding and Offboarding

In order to ensure the highest level of service for our clients, CGI believe that by working with our clients to fully understand the backend services and end user experience together the correct level of service can be achieved. The on-boarding experience is key to ensuring the correct level of IaaS infrastructure is provisioned to match against the service.

4.1. Onboarding

We excel in seamlessly onboarding and offboarding clients onto public and private cloud infrastructures and services, particularly within the Public Sector. Leveraging proven skills, tools, and methodologies, we ensure a smooth transition process that minimises disruptions and maximises efficiency.

CGI will apply its standard transition methodology which has been used in all service on- and off-boarding'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 Onboarding is achieved through the following high-level steps:

- CGI will work with the client to ensure that the most effective and appropriate service is delivered to the end user community.
- CGI will assist potential clients in calculating the required compute and storage requirements along with appropriate additional services as required.
- Service templates are identified from the existing service catalogue, and a solution design is created.
- Service levels are selected to suit the SLA’s required.
- The requested services (virtual machines, storage, and network) are deployed.
- CGI finalises the client’s configuration then provides connection details to enable application loading, administration, and rollout.
- A RACI is created as part of onboarding to determine ownership and accountability lines identified and communicated.
- Automation / capacity management / monitoring are all enabled to ensure that services are integrated into CGIs Service Desk and Control Bridge.
- Our services are simple to consume. New clients are asked to provide us with a list of authorised contacts and permission levels with whom we can engage, and those nominated individuals are provided with documentation and if necessary, training on how to contact us for support, how to access the ticketing and monitoring portals.

4.2. Offboarding

Service Offboarding is instigated by a client request or after expiration of the overarching CGI service agreement. Outside of these mechanisms, the minimum notice term would normally be 30 days’ notice in writing.

4.2.1. Decommissioning Process

For services provided on the CGI Public Sector Cloud platform, CGI cannot provide any form of certified destruction due to the shared nature of the underlying hardware infrastructure. However, the client is free to

© 2026 CGI IT UK Ltd

move their data away from our service at any time and once notified, CGI will remove all client data from the platform using the standard platform tools.

4.2.2. Access to data upon exit

If a request to export data from the cloud service is requested, all client data held will be exported and made available using appropriate media (supplied at the client's cost), in line with the security classification of the data and information management policies in force.

Charges for this service are dependent on the volume and complexity of the data required and will be estimated on a case-by-case basis. Additionally, if the client wishes to have copies of the virtual machines for deployment for example into another cloud, these can be securely exported in the OVF format via SSL. ISO images can also be securely downloaded via SSL. After notification that data has been successfully recovered and is complete, CGI will purge client data from any compute or storage device / media that remains part of CGI estate.

If no data export from the Cloud Service is requested, deletion of any virtual machine image and data will occur in line with the service agreement. If no service agreement is in place, all associated data will be deleted within five working days of service termination.

Please note that clients will not be granted hypervisor level access to CGI Public Sector Cloud platform for data migration purposes.

4.3. Cloud Security Principles

The UK National Cyber Security Centre (NCSC) was set up to improve the underlying security of UK public services and public sector IT from cyber-attacks as more and more organisations adopt a cloud first strategy. Its 14 Cloud Security Principles are expansive and thorough and include such important considerations as data in-transit protection, supply chain security, identity and authentication and secure use of the service, allowing service providers like CGI to highlight the security benefits of our products and services in an easily consumable format. The table below details the CGI response to each of the 14 NCSC Cloud Security Principles:

Cloud Security Principle	Description	Why this is important	Response
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	CGI have and maintain the following: PSN assured services. TLS (HTTPS or VPN) version 1.2 or later protocols Encrypted PSN services Bonded fibre optic connections
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage, or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.	CGI have and maintain the following: NCSC and CPNI-approved erasure process Secure containers, racks, or cages Physical access control policy in all our datacentres

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	CGI's community cloud delivered to government clients is for the use of UK public sector clients only. CGI securely separate consumer data and services from other consumers of the service. CGI's management of a consumer's services is kept separate from other consumers. CGI provides both commercial/enterprise and secure public sector OFFICIAL IaaS environments. These environments are kept both logically and physically separated, with separate physical servers used to host the OFFICIAL environment. When a new client organisation is created, it is placed in either the commercial/enterprise area or in the OFFICIAL environment subject to requirements, with a unique vOrg, associated unique virtual firewalling and contexts and separate storage resource pools. This combined logical and physical separation ensures that no clients are ever able to jeopardise the information security requirements of the others. These separation methods are tested / proved as part of the ITHC scope.
4. Governance framework	The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	CGI have an ISMS in support of our ISO 27001:2013 certification to ensure the security of both our own and our clients' data is secure.
5. Operational security	The service provider should have processes and procedures in	If this principle is not implemented, the service can't be operated and	Configuration and change management – CGI operate an ITIL aligned and ISO 27001

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
	place to ensure the operational security of the service.	managed securely in order to impede, detect, or prevent attacks against it.	validated Change management policy. Vulnerability management – CGI operate a patch and vulnerability management policy, in-line with ISO 27001:2013 / PCI-DSS Cyber Essentials controls to ensure the confidentiality, integrity, and availability of its data and that of client data stored on its systems. Protective monitoring – CGI ensure all 5 key aspects of protective monitoring: Business traffic crossing a boundary. Activity at a boundary Alerting on events Accurate time in logs Data backup status Are conducted on our secure government IaaS platform. Incident management - CGI operate an ITIL aligned and ISO 27001 validated Incident management policy.
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	At a minimum, staff have the following background checks conducted: Identity and Right to Work checks. Residency Verification (UK and abroad) 5-year employment checks BPSS Checks Credit Check All engineers with access to public sector systems have the following: Employment history (minimum 5 years) Educational background (back to higher education) BPSS check (engineers only) Address history (6 years) Electoral Role check

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
			Credit Check Directorship search Identity/Right to Work check. Residency Verification (UK and abroad) Two-character references SC Clearance (on-going)
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	CGI develop and implement formal, documented configuration standards for its information systems. CGI's Hardening Guides detail the procedures in use. All remote logins that enable administrator access to CGI information systems storing, transmitting, or processing sensitive data must be encrypted. CGI have a formal, documented process to identify newly discovered security vulnerabilities and update CGI configuration standards to address new vulnerabilities.
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	CGI uses a number of suppliers who provide services and goods. The effective management of these suppliers is essential in the provision of onward services to our clients and ensuring the security of our systems and data. The level of management and control applied is appropriate to the significance and value of the services being supplied, and to the level of security required. For example, an ad hoc supplier of stationery does not require the same level of control as a supplier providing ongoing technical services. Suppliers will be required to provide evidence that demonstrates they have the ability to supply the service, maintain the

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
			service levels, and meet any security requirements. For Category 1 Suppliers who are not ISO 27001 certified an audit programme will be established and agreed such that through annual audits all key areas are audited at least every 3 years.
9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications, and data.	CGI have secure password policies in operation on all its publicly accessible systems, using tools such as 2 factor authentication and complex password policies. This includes all systems used in the provision of our services, including our ITSM portal, vCloud director and other associated tooling.
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	Connection to the CGI OFFICIAL IaaS is by encrypted VPN connection only, with 3 factor authentication. All clients are required to complete a client contact list with associated levels of authorisation. The client is in control of this list, with only tier 1 contacts able to make changes. Where clients call by telephone from an unknown number or request major Changes, CGI have a secure password agreed with each client in advance to authenticate that user.
11. External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	Connection to the CGI OFFICIAL IaaS is by encrypted VPN connection only, with 3 factor authentication. The controls listed in section 9 and 10 ensure no other external method of access is possible without appropriate authentication being achieved.
12. Secure service administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	CGI operate a strictly monitored and robust secure access control policy for all service administration tooling, including the following: Password-Based Access Control - Any system that manages either critical or sensitive information

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
	exploitation that could undermine the security of the service.		must utilise a properly maintained version of an approved password-based access control system. This system should have the ability to log both successful and unsuccessful authentication requests. Role-Based Access Control Privileges - The information systems access privileges of all users must be defined based on their officially assigned roles within CGI. This is defined within the CGI Access Authorisation Matrix spreadsheet. Centralised Access Control - CGI maintain an unambiguous, organised, and current record of all production information system access privileges. Default to Deny - Access to all of CGI's Public and Critical servers will only be granted if explicit access controls have been defined. Operating System and Application server subsystems will be set to a default that blocks access by unauthorised users. All access attempts that are unsuccessful will be recorded and logged. CGI conduct an annual ITHC, including several days of internal penetration testing, to ensure that no access is possible to any of CGI's management systems from an unauthorised threat actor. Weekly internal scanning ensures that CGI maintain the highest level of security on our management systems.
13. Audit information	Consumers should be provided with the audit records they need to monitor access to their	If this principle is not implemented, consumers will not be able to detect and respond to	The CGI internal logging platform is a collection of servers and tools designed to capture critical logs and process these to identify any

© 2026 CGI IT UK Ltd

Cloud Security Principle	Description	Why this is important	Response
provision to consumers	service and the data held within it.	inappropriate or malicious use of their service or data within reasonable timescales.	irregularities as well as troubleshoot issues. CGI will provide audit and logging information on request to clients if required. However, clients are responsible for implementing their own logging and auditing on their services above the hypervisor.
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	CGI provide the VPN client/token to access our secure OFFICIAL IaaS from whichever device/user the tier 1 authorised users at the client define. The consumers of CGI's services are responsible for ensuring that their own end-point devices are secure when accessing the service.

Table 11 - Cloud Security

5. Service constraints.

5.1.1. Maintenance

Sometimes it is necessary to undertake maintenance, when that happens it is the job of the support team to help the client to minimise the impact of any maintenance activity on the delivery of services to end consumers.

Maintenance includes all regularly scheduled error corrections, third party software updates and upgrades to the CGI hardware. Some maintenance can be conducted without risk to client services; CGI will undertake this background maintenance at its discretion from time to time.

Occasionally we will need to suspend the service for a planned outage where maintenance cannot be conducted by any other means. Planned outages will be performed between the hours of 12am and 8am and we will provide the client with seven days' notice of any planned outage.

In extreme circumstances CGI may need to interrupt the Services to perform emergency maintenance, this will only happen where it is unavoidable to ensure the on-going delivery of service or where there is a risk to client data or system integrity.

6. Service Levels

6.1.1. Performance

Resources are guaranteed to perform materially in line with the specification.

6.1.2. Availability

Virtualised IaaS services come with a 99.99% uptime target. Physical IaaS services come with a 99.9% uptime target.

© 2026 CGI IT UK Ltd

6.1.3. Support Hours

Support is provided to Clients to help them derive the best value possible from the Services and is available 24x7x365 by phone through our service desk, via our ticketing portal and via e-bonding with your ITSM tool of choice.

6.1.4. Severity Definitions

Support is provided to Clients to help them derive the best value possible from the Services and is available 24x7x365 by phone through our service desk, via our ticketing portal and via e-bonding with your ITSM tool of choice.

Priority	Description	Response time	Target resolution time
Priority 1	The Service is 'down' and inaccessible or has suffered from failures which significantly degrade service and reduce functionality to all users. Priority 1 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the CGI Emergency support Line. 24x7x365	Four Hours, 24x7x365. Continuous effort after initial response and with Client co-operation. One Hour for Non-virtualised Infrastructure resolution where a Hot Spare Device has been purchased.
Priority 2	Operation of the Services is severely degraded or Single Points of Failure have resulted from failures. Service to users is not affected. Priority 2 incidents shall be reported by telephone only.	Within 30 Minutes of completing a call to the CGI Emergency support Line. 24x7x365	Four hours from the start of the next business day unless an escalation to Priority 1 is requested.
Priority 3	Certain non-essential features of the Service are impaired while all major components of the Service remain functional. Priority 3 incidents are to be reported via the ticketing system.	Within 1 Normal Business Hour.	Within seven Business Days after initial response.
Priority 4	Errors, bugs, or inconsistencies that are not service affecting and clearly have little or no impact on the normal operation of the Services. Priority 4 incidents are to be reported via the ticketing system.	Within 24 Normal Business Hours.	As determined during the investigation of the incident.

Table 12 - Severity Definitions

© 2026 CGI IT UK Ltd

6.2. Service Management

CGI provides service management to its clients based on the ITIL framework. Service delivery management is delivered by a team of experienced professionals who provide regular reporting, technical account management and a regular review of business objectives to ensure the service is delivering the business value expected. The standard service delivery report provides information on incidents, changes and other business events that might impact or change the service.

The following sections detail how we monitor and support the environments.

6.2.1. Utilisation monitoring

We use commonly available open-source tooling to provide monitoring and reporting. The output of that reporting is available in real time in our portal as well as being available as data feeds that can be consumed by clients.

6.2.2. Support

Support is provided to clients to help them derive the best value possible from the services and is available 24x7 by phone through our service desk for critical issues. For non-critical issues support is available through our ticketing portal.

6.2.3. Detailed Service Description

Service Feature	Description	Client obligations	Limitations
24x7 P1 failure support	24x7 Telephone support for priority 1 issues.	Clients must ensure that contact detail lists are up to date. Priority 1 issues must be reported by Telephone.	Support is limited to P1 infrastructure failures.
9-6 business day support	Business hours telephone and ticket-based support for priority 2-4 issues.	Clients must ensure that contact detail lists are up to date.	Support is limited to P2-4 infrastructure failures.
Network Changes	Changes to network services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	The number of changes per month is limited.
Server Changes	Changes to Server services will be carried out in line with the change management procedure	Clients must provide all the details needed to ensure changes can be made.	

Table 13 - Detailed Service Descriptions

7. After sales support

Technical support for our Public Cloud Hosting Service is provided on a 24x7x365 basis via our Service Desk. With regards to Service Management (ITSM) and service levels our approach is articulated in section 6 above.

© 2026 CGI IT UK Ltd

8. Technical requirements

Our Private Cloud Hosting Service is provided as a Remote Infrastructure Management (RIM) service located from within our secured delivery locations in South Wales in addition to hosting locations located in the UK at Crown Hosting Data Centres. Subscribing to the service will require remote connectivity and detailed design which will be undertaken during initial requirements specification and service transition phase to meet the client's explicit needs.

9. Outage and maintenance management

9.1. Event Management

Our Private Cloud Hybrid Cloud Management Platform (HCMP) provides alerts and automated incident ticketing for hosted infrastructure using direct integration with our ITSM Platform and our Digital Command Centre. Optionally we can integrate event alerting with the client's ITSM toolset as an additional cost during service transition.

9.2. Scheduled Maintenance

Maintenance Windows

Our Technical and Service Management Teams will communicate with the client's stakeholders to confirm the cloud provider's maintenance schedules, including planned maintenance windows when the provider performs maintenance tasks that may impact service availability.

Impact Assessment and Communication Plan

Our Technical and Service Management Teams will impact assess scheduled maintenance activities potentially effecting your services and will communicate this information 24 hours prior to the maintenance window occurring.

They will provide regular updates on maintenance schedules progress and any changes to the plan to always ensure operational visibility.

10. Hosting options and locations

CGI provide Private Cloud hosting services from UK sovereign Crown Hosting Data Centres in-line with the Government Security Classification Policy.

Our Private Cloud Hosting Service is operated remotely from within our secured delivery centres located in South Wales.

11. Security

Our service adheres to rigorous security standards to protect government data from unauthorised access, data breaches, and cyber threats. We ensure that the relevant compliance certifications and attestations are in place that demonstrate their adherence to government standards and regulatory requirements, such as Cyber Essentials, ISO/IEC27001, National Cyber security (NCSC), GSCP and GDPR, in addition to any specific certifications required by UK government agencies.

© 2026 CGI IT UK Ltd

12. Service Pricing and Terms and Conditions

12.1. Pricing

Please refer to the associated Pricing Document relevant for this Service.

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:

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.

© 2026 CGI IT UK Ltd

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:

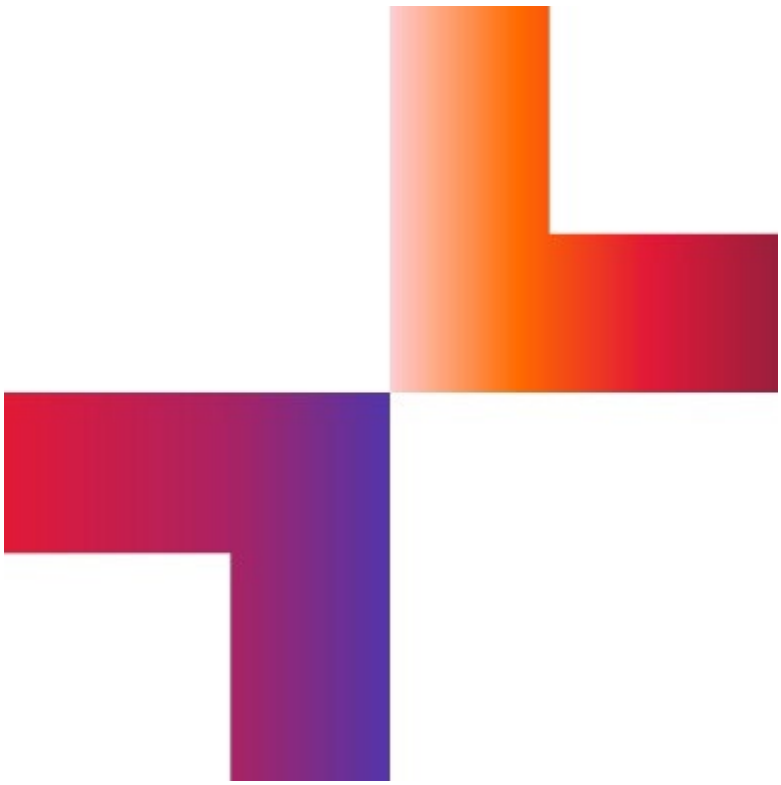
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk