



Managed Network Services

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	5
2.	Data backup and restore	11
3.	Service Continuity	11
4.	Onboarding and Offboarding	12
5.	Service constraints	13
6.	Service levels	15
7.	After sales support	17
8.	Technical requirements	18
9.	Outage and maintenance management	18
10.	Security	18
11.	Service Pricing and Terms and Conditions	19
12.	Further information	19
PROPRIETARY AND CONFIDENTIAL		21

Service Definition overview

While traditional outsourcing was driven by cost reduction, today's organisations seek a trusted partner who can also increase agility, resilience, and innovation in an increasingly complex digital environment. At CGI, we refer to outsourcing as managed services—because we work as a true extension of your organisation, delivering outcomes, not just operations.

CGI's Managed Network Services provide secure, high-performance connectivity across your branch sites, data centres, and cloud environments. We deliver full lifecycle management—from design and deployment to 24/7 monitoring and optimisation—ensuring your network is scalable, resilient, and future-ready.

Our service integrates enterprise-grade infrastructure with real-time visibility, automation, and proactive support. Delivered from our UK-based Digital Command Centre and aligned to ITIL standards, CGI's approach ensures continuous improvement, operational efficiency, and strong governance.

We go beyond network maintenance—helping you build the robust IT supply chain required to accelerate innovation, enhance user experience, embed security, and optimise operations. Whether refreshing legacy networks or supporting new deployments, CGI offers a fully managed, software-defined solution tailored to your needs—combining deep expertise, modern tooling, and a partnership approach.

Features

- Fully managed network services from leading vendors including Fortinet, Cisco, HPE Aruba / Juniper, F5 and Zscaler.
- End-to-end service: network surveys, design, deployment, patching, and updates.
- Integration with hybrid/multi-cloud environments.
- 24/7 UK-based monitoring and incident response via single-pane-of-glass view and integrated into our ITSM ServiceNow platform.
- Advanced analytics, AIOps, and real-time performance insights.
- Support for IoT, secure remote access, and zero-trust security architectures.

Benefits

Choosing CGI as your Managed Network Services partner will deliver measurable impact across your organisation:

- Enhanced performance – Our optimised network infrastructure, designed and implemented by experienced, certified CGI network architects, ensures high-speed, reliable connectivity that drives improved digital experiences and boosts user productivity.
- Scalable agility – CGI has experience in enabling rapid service expansion across sites, devices, and workloads, adapting to your evolving operational needs with ease.
- Reduced risk exposure – We help minimise operational risk and technical debt through proactive vulnerability management, scheduled patching, and the oversight of end-of-life hardware and software, supporting long-term infrastructure resilience.
- Operational efficiency – We streamline event management and incident response through our AIOps and centralised tooling, reducing manual workload and accelerating time to resolution.
- Focus on strategic priorities – Our fully managed service allows your internal IT teams to shift focus to transformation and innovation, rather than day-to-day operations.
- CGI's proven expertise – Backed by over 25 years of experience, our UK-based team of certified professionals leverages strong partnerships with our vendors to deliver secure, enterprise-grade solutions.

Why CGI?

A managed network from CGI will ensure that together we can help you obtain a competitive edge. Our 50 years' experience in business and IT consultancy ensures that we have the experience and vision to develop

new networks to mirror your business function and outcomes, offering insight into application performance and user experience.

CGI has over 25 years of experience providing fully integrated, managed network services built to enable our clients' best possible performance. We have our own UK network services practice and have relationships with all major carriers and network equipment vendors, designing and supporting major networks for large public and private sector clients.

We optimise our client's service, seeking savings through vendor consolidation and using next-generation software-defined services that reduce the time and effort needed to build and maintain the network. CGI is trusted to manage networks for more than 80 clients across secure government and commercial clients. We support more than 2,000 WAN links, over 20,000 physical LAN devices, and hundreds of physical and virtual managed firewalls.

Our network services are provided from our centralised Digital Command Centre located at our 24/7/365 UK Control Bridge, supported by local engineering and service delivery resources. The Control Centre serves as a centralised hub to monitor, control, and operate business-critical infrastructure enhanced by CGI's AIOps platform, which applies automation and intelligent event correlation to drive faster incident resolution and improve service availability.

Our operations teams are supported by a pool of project architects and engineers who work closely with our clients to design and deliver project-initiated change activities. CGI professionals are certified with all main technology vendors. We are a Cisco Cloud and Managed Services Advanced Partner, Fortinet Expert Level, and a Microsoft Gold Certified Partner.

We balance the need to transform networks whilst proving a stable service by ensuring interoperability of new technology with old technology and associated management platforms. We avoid big-bang implementations through using proof of concept, pilot sites and rigorous testing all supported by our dedicated project management and network architect teams.

1. Service Description

1.1. Overview

CGI is a trusted long-term partner for the design, deployment, and ongoing management of secure, high-performance network services. As a network integrator, we have delivered and supported major infrastructure programmes for large public and private sector clients—spanning complex, highly secure environments to multi-site commercial estates. Our clients rely on us not only to manage operations but to shape their future connectivity strategy through innovation and collaboration.

We build strong, enduring relationships by aligning with each client’s technical, commercial, and organisational goals. From taking on existing estates to delivering full network transformations, our services are tailored to maximise efficiency and reduce complexity. We optimise service performance through vendor consolidation and by leveraging next-generation software-defined technologies—reducing the time, cost, and effort required to manage and evolve your network.

Figure 1 below displays our managed network service portfolio.



Figure 1. CGI Managed Network Services

1.2. Telecoms Order Management - Simplifying Network Delivery

As part of CGI’s Managed Network Service offering, clients benefit from our dedicated Telecoms Order Management (TOM) capability, providing a single, expert coordination point for all telecoms activities required to deliver and maintain the end-to-end network service. By centralising this function, clients avoid the complexity of managing multiple telecoms providers themselves and gain a more streamlined, predictable delivery experience.

Acting as the client’s managing agent, the TOM team manages the full lifecycle of telecoms orders — including new circuits, bandwidth changes, equipment requests, and service migrations — through a structured change control process. This includes validating requirements, placing orders with approved suppliers, tracking progress, and ensuring that installations, surveys and engineering activities are delivered on time and to expectation. This proactive management approach helps shorten delivery timelines, reduce delays, and remove administrative burden from client teams.

In addition to order management, CGI TOM provides robust performance oversight across all telecom’s suppliers. The team conducts regular service reviews, monitors adherence to delivery targets and service levels, manages escalations, and ensures telecoms billing is accurate and aligned with contracted rates. This gives clients improved visibility and control across a multi-vendor landscape, enhances supplier performance, and supports stronger cost assurance through accurate and transparent billing validation.

1.3. CGI's Managed Networks Portfolio

CGI offers a comprehensive suite of managed network services designed to deliver secure, scalable, and high-performing connectivity across your organisation. Whether you're looking to optimise existing infrastructure or deploy new, software-defined solutions, our services are tailored to meet your evolving needs and drive long-term value. The table below outlines our core managed service offerings.

Service	Description	Vendors
Managed WAN	CGI's Managed WAN Services deliver secure, high-performance connectivity across your organisation's sites, supporting critical communications between branches, data centres, and cloud platforms. We design, procure, and manage fully tailored WAN solutions, including MPLS, direct internet access, dark fibre, SD-WAN, and dedicated cloud connect services—ensuring a reliable foundation for modern digital operations. Our partnerships with leading telecom providers enable us to match each location with the most effective, value-driven connectivity options. From discovery and network design through to deployment and 24/7 operational support, CGI provides full lifecycle management. We leverage automation, QoS policies, and centralised monitoring to enhance performance, prioritise key applications, and ensure secure, resilient data transport. Whether you're expanding your estate or optimising legacy infrastructure, CGI's WAN solutions are built to scale with your business—improving agility, reducing complexity, and supporting seamless cloud integration.	Vodafone, BT, Virgin Media, Commsworld, Gamma
LAN & Wi-Fi	CGI's Managed LAN and Wi-Fi services deliver fast, secure, and reliable connectivity to support your business-critical operations across campuses, branch offices, and hybrid workplaces. From design and deployment to 24/7 monitoring and optimisation, we provide an end-to-end service tailored to your specific environment. Whether modernising legacy infrastructure or deploying new network capabilities, our experience ensures each solution is right-sized, resilient, and aligned to your performance, security, and scalability needs. With CGI, you gain more than just connectivity, you benefit from intelligent network insights, proactive issue resolution through AIOps, and seamless device onboarding via zero-touch provisioning. We will integrate identity-based access, zero trust principles, and modern wireless standards to help create a network that's ready for future demands, without compromising today's reliability.	Cisco, Meraki, HPE Aruba, Fortinet
Managed Firewall	CGI's Managed Firewall Services provide comprehensive protection for your network perimeter—whether at the data centre, branch office, or in the cloud. We deliver end-to-end firewall design, deployment, and management services using industry-leading platforms such as Fortinet, Cisco, Palo Alto, and Checkpoint. Our approach ensures your firewall solution is tailored to your business environment, compliance requirements, and evolving threat landscape. With 24/7 monitoring, automated patching, ruleset optimisation, and secure configuration management, CGI ensures your firewall estate	Fortinet, Palo Alto, Checkpoint, Cisco

Service	Description	Vendors
	is always up to date and operating efficiently. We support both physical and virtual appliances and can extend your security coverage with web application firewalls, DDoS protection, and load balancers. All services are managed from our UK-based Digital Command Centre, backed by our third-line specialists and delivered with a focus on availability, auditability, and long-term resilience.	
Unified Communications and Contact Centre	CGI delivers integrated Unified Communications (UC) and Contact Centre solutions that connect people, systems, and channels to improve customer experience and operational efficiency. From traditional VoIP telephony to modern, cloud-hosted UCaaS platforms, we help organisations evolve their communications landscape with scalable, secure, and feature-rich services. Our offerings include seamless integration with Microsoft Teams, enabling voice, video, and collaboration tools within the enterprise productivity suite. For customer engagement, we deploy cloud-based contact centre (CCaaS) platforms with open APIs—allowing integration with CRM systems and ITSM platforms for enhanced service automation and user insight.	Ringcentral, Avaya, Genesys, Maintel, Ribbon, Cisco, Microsoft Teams
Data Centre Network Services	CGI designs and manages modern data centre networks built for high performance, agility, and security. Our solutions leverage software-defined fabric and leaf-spine architecture to deliver low-latency, scalable connectivity that supports today's dynamic workloads and hybrid infrastructure models. We integrate advanced features such as virtualised firewalls, load balancers, and Hardware Security Modules (HSMs) to provide robust perimeter and internal protection. With automation, centralised policy management, and deep visibility, our networks enable efficient operations and resilient, future-ready infrastructure.	Cisco, F5, Dell, Fortinet
Public Cloud Landing Zones	We design and manage secure, scalable landing zones for public cloud environments enabling organisations to accelerate digital transformation while maintaining control, compliance, and performance. Our landing zone solutions establish a robust cloud foundation, incorporating automation of network segmentation, firewalls, web application firewalls (WAF), load balancing, and network security groups (NSGs) to protect critical workloads from day one.	Azure, AWS, Oracle, Fortinet, F5
SD-Branch	CGI's Software-Defined Branch (SD-Branch) services simplify and secure branch connectivity by converging WAN, LAN, Wi-Fi, and next-generation firewall technologies into a single, centrally managed platform. Designed and delivered using industry-leading solutions—such as Fortinet's Security Fabric—our SD-Branch approach enables consistent policy enforcement, improved visibility, and enhanced user experience across distributed environments. From design and deployment to ongoing management and support, CGI helps organisations streamline branch operations, reduce infrastructure complexity, and scale securely. Our SD-Branch solutions include zero-touch deployment, cloud integration, anomaly detection, and performance optimisation—backed by 24/7	Fortinet, HPE Aruba

Service	Description	Vendors
	monitoring from our UK Digital Command Centre. Whether you're refreshing legacy infrastructure or enabling agile expansion, SD-Branch delivers a flexible, resilient, and secure foundation for your connected enterprise.	
SD-Access	Our Software-Defined Access (SD-Access) service transforms how organisations manage network access by applying identity-based, zero-trust policies across wired and wireless infrastructure. Built on software-defined networking principles, SD-Access reduces operational overhead while enhancing network performance, scalability, and security. Our service includes dynamic policy enforcement, seamless device onboarding, real-time analytics, and simplified network segmentation. Delivered via our UK Digital Command Centre and aligned to ITIL practices, CGI's SD-Access service provides a future-ready network foundation enabling secure, efficient access at scale across branch, campus, and hybrid environments.	Cisco
Secure Service Edge / Secure Access Service Edge	CGI's SSE/SASE services provide a unified, cloud-native solution that combines secure connectivity with advanced security controls enabling secure, policy-driven access to applications, data, and services across any location or device. Built on a zero-trust foundation, SASE integrates SD-WAN with key SSE technologies including ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Firewall-as-a-Service (FWaaS). Designed for the hybrid enterprise, CGI delivers end-to-end SSE/SASE services covering assessment, design, deployment, and ongoing management. Our solutions replace legacy VPNs, simplify policy enforcement, and support cloud-first strategies with scalability and visibility.	Zscaler, Fortinet
24x7 Managed Service	South Wales based Digital Command Centre backed by our award-winning service desk.	UK-based network engineers
AIOps	Our version of AIOps is built on container-based architecture using open-source tooling pulling data in from tools like Zabbix, Cisco Catalyst Centre and FortiManager and combining that with incident information from ServiceNow to enable faster response and automated ticket enrichment.	CGI developed technology

1.4. Managed Network Service Considerations

1.4.1. Wired Networking

1.4.1.1. Wide Area Network

CGI provides managed Wide Area Network (WAN) services where we have implemented the network, or where the design aligns with our supported architecture. This enables us to deliver a consistent, high-quality service across all managed sites.

In cases where a third-party network provider is contracted directly by the client, CGI can provide complementary support through coordinated incident management and service liaison. This includes administrative support such as inventory reviews, connectivity ordering, and third-party engagement to help

maintain service continuity. Where reporting is required beyond standard scope, we're happy to discuss tailored reporting options to suit your operational needs.

1.4.1.2. Local Area Network

CGI provides managed Local Area Network (LAN) services where the infrastructure is either designed and deployed by CGI or aligns with a supported architecture. This allows us to deliver reliable, scalable management tailored to your environment.

To manage devices effectively and provide proactive support, SNMP compliance is required. Devices without SNMP capabilities can still be supported on a limited break/fix basis, and we'll collaborate with you to define the appropriate management approach for these assets.

1.4.1.3. Service Variations

Our managed network service is designed to provide comprehensive support for day-to-day operations. Certain activities and components typically fall outside the standard service scope, as they are often delivered during the initial transition or are managed separately by agreement. These include:

- Bespoke or exception-based reporting, where additional setup may be required.
- Initial network installations, generally covered during the transition phase.
- Circuit rentals and telecoms provider charges.
- Software licences, upgrades, and patching outside of standard schedules.
- Hardware and software maintenance for third-party or client-owned assets.
- Significant moves, adds, or changes—particularly where this involves site attendance, third-party coordination, infrastructure expansion, or after-hours work.
- Consumables (e.g., cables, power adapters).
- Optional 24x7 remote support, which can be included based on specific contract requirements.

CGI will always work with clients to scope these elements as needed, ensuring transparency and alignment with operational and commercial expectations.

1.4.2. Wireless Networking

1.4.2.1. Wireless LAN

Before deploying a Wireless LAN solution, a few key considerations must be addressed to ensure successful and secure operation within your environment. These include:

- A wireless policy statement covering usage and deployment (CGI can provide a recommended template).
- Confirmation of environmental suitability and safety for wireless deployment.
- Outcomes from a site survey to inform design and placement.
- Preferred vendor or manufacturer selection for access points.
- Security controls aligned to organisational requirements.

To support effective deployment, CGI recommends a site survey. Two options are available:

- Basic survey – Provides indicative access point locations based on predictive modelling. Suitable for initial planning but does not guarantee coverage or security.
- Comprehensive survey – Includes on-site measurement, aerial placement, and a detailed report with validated coverage, security posture, and deployment recommendations.

Survey pricing is available on request, and we will work with you to determine the most appropriate approach for your organisation.

1.4.2.2. Service Variations

Our managed Wi-Fi services are designed to support ongoing network availability and performance. Certain activities or components typically fall outside the standard service scope and are addressed as part of initial deployment or as tailored service elements:

- Wireless site surveys and installation readiness activities.
- Software licences, feature upgrades, and patching outside standard schedules.
- Maintenance of third-party hardware or software not within CGI's management scope.

- Complex moves, adds, or changes involving site visits, third-party coordination, or additional infrastructure.
- Work required outside of agreed support hours.
- Consumables (e.g., mounting kits, cables, antennas).

We'll work closely with you to review these elements and ensure they are planned and supported effectively as part of a complete service model.

1.4.3. Managed Security Services

1.4.3.1. Firewall

CGI provides full lifecycle management of enterprise and next-generation firewall environments, including design, deployment, rule set management, monitoring, and policy tuning. Our service includes key features such as intrusion prevention (IPS), deep packet inspection, SSL inspection, web filtering, application control, and logging aligned to your organisation's security standards, risk posture, and business requirements.

We work in close partnership with your security teams to ensure that firewall policies reflect current threat landscapes and operational needs. All management activities follow a defined change control process, ensuring traceability and compliance.

The applicability of this service typically includes the following:

- The service applies where CGI has designed and deployed the firewall architecture, or where the environment conforms to CGI-supported designs.
- Security policy ownership rests with the client; CGI will implement and manage firewall rules in accordance with authorised instructions and change processes.
- We can interface with your internal SOC, a third-party SOC, or provide a managed SOC capability from CGI, ensuring alignment on threat detection, incident response, and policy enforcement.
- Protective monitoring and vulnerability management such as updating IPS signatures or tuning inspection rules require agreed input from the client or nominated SOC authority (CGI or third party).
- We work collaboratively to review and maintain security rule sets, ensuring they are current, effective, and in line with your governance model.

This approach ensures that your firewall infrastructure is proactively managed, policy-driven, and seamlessly integrated into your broader security operations.

1.4.3.2. Service Variations

CGI's managed firewall service is designed to provide proactive, secure, and policy-aligned support for your network perimeter. Some activities or components typically fall outside the core managed service scope and are addressed during project transition or managed through specific service arrangements. These include:

- Renewal or reinstatement of lapsed licences and vendor maintenance.
- Initial installation and deployment, typically covered in the transition phase.
- Software licences, feature upgrades, or out-of-scope patching.
- Maintenance for hardware or third-party software not managed by CGI.
- Major moves, adds, or changes—especially where this involves on-site activity, external party coordination, or significant infrastructure changes.
- Consumable items, such as cables or rack components.

We'll work closely with you to ensure these elements are clearly understood and integrated where appropriate into your overall support model.

1.5. Monitoring and Reporting

The table below describes the standard reports and reporting period included under the CGI Managed Network Service.

Type of Monitoring / Tooling	Reporting Period
Network Performance Monitoring	Monthly

Type of Monitoring / Tooling	Reporting Period
Network Bandwidth Analysis	Monthly
Network Configuration and Change Management	Monthly
Topology Mapping and discovery	Monthly
Real time monitoring	24x7
Incident and event management	24x7
Problem management	8x5

Table 1 - Reporting Types and Periods

Additional or alternative reports can be provided by exception. Where bespoke reporting is required, any setup or ongoing effort—particularly may be subject to additional commercial consideration, which will be discussed and agreed in advance.

1.6. Third Party Management

Our standard service includes liaison with third parties who maybe sub-contracted to provide service and/or maintenance on elements of the client network. This liaison may include the following activities which CGI can perform for the client:

- Reporting of faults, problems, and incidents to third parties and follow up processes until resolution.
- Periodic supplier review meetings.
- Negotiation of contract values and procurement of additional services and/or support.
- Moves and changes that will involve third parties.

2. Data backup and restore

All CGI essential and critical systems and information (including any personal data) is backed up (including client information stored in CGI's owned or shared environment) in accordance with CGI's backup standard, ensuring the capability of full restoration of data if needed. Backup media is encrypted and stored off site using trusted storage suppliers.

Any further requirements (e.g. contractual and/or legal requirements) for the erasure of personal data contained in information held for backup requirements, is recorded in specific contractual arrangements, where the personal data-specific responsibilities are dependent on the client. Contractual arrangements will also include as required:

- Informing the client of any limits of the service regarding backup.
- Where CGI explicitly provides backup and restores services to clients, they are provided with clear information about their capabilities with respect to backup and restoration of personal data.
- If the jurisdiction imposes specific requirements regarding the frequency of backups of personal data, the frequency of reviews and tests of backup, or regarding the recovery procedures for personal data, CGI aims to demonstrate compliance with these requirements.

3. Service Continuity

We are ISO:27001 and ISO:22301 certified and maintain a corporate business continuity plan, supporting ITDR and ITSC. CGI has a dedicated Business Continuity Manager (BCM), who ensures that all services and contracts have a service continuity plan, reviewed, and updated at least annually and logged centrally.

In addition, technical recovery plans are prepared for each centralised service. Each service and site conduct a full BC test at least annually and often more frequently. The BCM compiles and communicates a quarterly

report to all client services, which includes BC and DR testing, and any lessons learned to enable knowledge sharing.

Our primary delivery location sits within our Data Centre complex, as a result it benefits from the same levels of security and service resilience that a modern Data Centre provides. The site is protected by backup power, high-capacity data communication links supporting high availability and mature Business Continuity plans.

Members have laptops and are equipped to work from home, receiving the same level of support and monitoring as our primary delivery location. If the site is compromised, our members will return home to work, updating telephony routing remotely to redirect traffic to alternative locations.

3.1. Business Continuity

Our approach to business continuity ensures that we can continue to operate throughout disaster scenarios and enables us to deliver a continuous, high-quality service for our clients.

We operate to a UK BCMS, with associated templates, audited and certified to ISO:22301 (the international Business Continuity standard) and designed to align with the Business Continuity Institute Good Practice Guidelines (2018).

We maintain a UK Business Recovery plan, which defines roles and responsibilities for the UK Business Recovery Team (BRT) – managing events 'on the ground' and a UK Crisis Management Plan, operating at the top level in CGI.

Each CGI site has a Facility Continuity plan, and each shared service team has a Service Line Continuity plan - which deals with all aspects which are relevant to the team's services (such as people, skills, information, systems, premises, suppliers) and the strategies and recovery processes covering them.

Our emergency procedures cover risks including fire, bomb/terrorist threat, flood/natural disasters, and pandemics, as well as IT incidents such as virus or malware attacks.

Communications in a disaster include notification to clients via our client engagement managers, to senior managers in CGI, and externally via our Corporate Communications unit.

4. Onboarding and Offboarding

4.1. Onboarding

CGI has proven and effective on and off-boarding skills, tools, and methodologies. We have successfully transitioned numerous Public Sector clients onto our managed network service. CGI has a dedicated team of managers who specialise in transition and who apply considerable previous experience in this area. 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.

4.2. Offboarding

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

Cease notices should be provided with a minimum of four calendar months as this allows formal notice to be served on sub-contracted suppliers who usually have a cease notice of three calendar months or 90 days. Where contracts with suppliers specify duration and/or cease notice periods that extend beyond this, then the notice period of the subcontractor will prevail.

Cessation penalties may apply for any cease notice within contract term. These and reasonable incidental costs will be passed to the client where applicable.

4.2.1. Access to data upon exit

Data retention periods and the handover or destruction of data at contract end will be specific to services consumed and vendor policy at the time that a service and components thereof, are agreed.

5. Service constraints

CGI's Managed Network Services are typically contracted for a minimum term of one year. Services will continue beyond the contract term unless notice is provided. CGI may revise pricing at renewal to reflect current commercial conditions.

All hardware and software licences procured as part of the service will be owned by the client upon delivery. CGI will support the configuration, management, and lifecycle of these assets as part of the managed service.

5.1. Supported Services

It is expected that on acceptance into service of network elements, those elements will:

- Conform to the preferred list stated below in Table 3
- The architecture/topology/technology is less than five years into deployment or is subject to a refresh programme led by CGI.

Category	Sub-Category	Technology
Wired Networking	Campus Switching	Fortinet FortiSwitch Cisco Catalyst
	Datacentre Switching	Cisco Catalyst and Nexus Series
	Routers	Cisco Catalyst Series and Fortinet FortiGate
Wireless Networking	WLAN	HPE Aruba Cisco Fortinet
Network Security	Datacentre Core Firewall	Fortinet FortiGate Cisco Firepower Checkpoint Palo Alto
	Datacentre Edge Firewall	Fortinet FortiGate Cisco Firepower Checkpoint Palo Alto
	Application/Layer 7 Firewall	Fortinet FortiWeb
	Branch Firewall	Fortinet FortiGate
	Public Cloud NFV/NVA	Fortinet FortiGate

Category	Sub-Category	Technology
	Public Cloud	Azure and AWS Firewall
	Public Cloud IPS	Fortinet FortiGate
Load Balancing	LTM	F5 LTM FortiADC
	DNS	F5 DNS
Unified Communications	Contact Centre (including CCaaS)	Mitel Cisco Genesis Avaya
Unified Communications	SIP	Circuits: Vodafone/Gamma/Virgin/BT SBC: Ribbon (Sonus)/Audiocodes/Mitel MBG
Unified Communications	IPT	Mitel Cisco Microsoft Teams
Remote Access VPN	RAS	Ivanti
Proxy Services	Web Proxy	Fortinet FortiGate
Authentication / 802.1x	Network Access Control	HPE Aruba Clearpass Policy Manager Cisco ISE FortiAuthenticator
Cloud hosted Security Service Edge	SSE / SASE	Zscaler Private Access / Zscaler Internet Access FortiSASE

Table 2 - Support Technologies

Should Network Virtual Appliances (NVA) be utilised to provide any of the above technologies, the client is responsible for providing and supporting compute infrastructure to support the virtual machine images.

5.2. Operational Scope

The managed service includes the following standard capabilities:

- Network monitoring, either 8x5 or 24x7 as required.
- Incident and problem management.
- Access to network spares or agreed hardware replacement service.
- Secure network access to support service delivery.
- Reporting against defined key performance indicators (KPIs).
- Software updates and patching in line with agreed processes.
- A defined service request catalogue and change management approach.

5.3. Direct Costs

The following activities are typically not included in standard support and are discussed separately during pre-sales or transition planning:

- Due diligence, transition, and transformation activities.
- Technology refresh, hardware purchases, and software subscriptions.

Significant moves, adds, or changes, including:

- Out-of-hours work or support at remote sites.
- Activities requiring third-party services (e.g. cabling, WAP installation).

5.4. Provisioning and Delivery

Service lead times are dependent on receiving complete and accurate information at the time of order. Orders may be subject to surveys, third-party dependencies, or landlord permissions. Delivery timelines begin from CGI's formal acceptance of the order, once all prerequisites are met.

5.5. Cancellation and Early Termination

Cancellations or significant amendments to placed orders may incur charges, particularly where third-party telecoms services are involved. Early termination may result in charges up to the full remaining contract value. Multi-year term discounts may also be subject to adjustment upon early cessation.

6. Service levels

CGI operates an ITIL compliant, award winning service management solution, a mandatory element of our service to ensure seamless delivery of service and ongoing support.

Services include:

- Continual Service Improvement
- 24x7 Digital Command Centre
- Major Incident Management
- Problem Management
- Change Management
- Availability and Capacity Management
- Service Level Management
- Configuration Management.

The CGI Digital Command Centre operates during normal UK business hours Monday to Friday and extends up to 24x7 subject to business need. Network support is facilitated by secure remote access. On-site attendance is provided subject to business need.

CGI will provide an event monitoring service as part of its overall Service Management responsibilities. CGI teams will monitor events generated through alerts from monitoring tools. Where the service desk is not a CGI provided service, incidents will be passed to and logged by the client's service desk.

Where CGI is not providing a remote hands service, SLAs will be subject to remote hands support by the client.

CGI shall collaborate with the client to investigate and seek root cause for any problems, with investigation being handled by CGI.

Several criteria define the applicability the services on offer. There are variances, exceptions, additions, limitations, and particular elements that are associated with individual services and will be peculiar to those services. Nonetheless, several common elements are evident in all services. These include, but are not limited to:

- The service is confined to instances where CGI has built the service offering or the service offering conforms to a design or architecture that CGI supports.
- Standard service based on accepted standard manufacturer infrastructure. Other manufacturer elements would be subject to review and separate negotiation.
- Standard service based on equipment that is currently maintainable, not approaching obsolescence, preferably less than five years old and has a forecasted useful life that exceeds the contract by at least one year.

- In instances where the Design Authority remains with either the client or alternative third party, the applicability of standard costs will be subject to a review and separate negotiation.

6.1. Service hours

Two levels of service hours are available:

- Standard Hours – covered by standard service and covering Monday to Friday, from 08:00 to 18:00, excluding UK Public Holidays.
- 24x7 – provided at an additional cost, this provides limited incident resolution service outside of Standard Hours with a cover of 24 hours a day, 7 days a week, 365 days a year.

6.2. Call Priorities

For WAN and hardware related incidents and problems, resolution times are dependent on the underlying support arrangements. CGI works with established carriers and hardware support partners to align service levels wherever possible, ensuring timely and effective incident resolution.

Severity		Definition	Users Impacted	Response from initial call being received	Resolution (See note)
P1	Critical	Total loss of service	All	30 Minutes	4 Hour
P2	Major	Major functionality unavailable with NO work round available.	Department or Location	1 Hour	8 Hours
P3	Minor	Major functionality unavailable with work round available.	Single User or Small group	4 Hours	24 hours
P4	Warning	Individual user affected	Single User	8 Hours	72 Hours
P5	N/A	Request for change, etc.	Subject to change request	As per agreed service request catalogue	As per agreed service request catalogue

Table 3 - Response and resolution times

6.3. Asset Ownership, licensing, and warranty

Where existing client services are brought into CGI's Managed Network Service, the client will be responsible for providing:

- Network hardware and software.
- Required software and subscriptions must remain licenced for the duration of the contract term.
- Valid hardware warranty or third-party break-fix support agreements must remain in place for the duration of the contract term, ensuring alignment with the required service level agreement.

Where Network hardware and software is acquired with CGI, ownership of these assets will be transferred to the client.

In instances where hardware warranty is no longer in place, or additional break-fix services are required, CGI can provide these services to ensure expedited replacement of any faulty equipment. SLAs will be backed by an appropriate spare holding, or a vendor / third-party support package acquired through CGI.

6.4. Obsolescence

On occasions, manufacturers/suppliers will announce equipment obsolescence. This will identify devices, and/or modules nearing end of life. This will result in the withdrawal of such devices from both development and ongoing support within a defined timescale. In such instances, CGI will inform the client and will serve formal notice of withdrawal of support within the timeframes outlined.

On long term contracts, where there is a risk of obsolescence before end of contract, caveats may be introduced into the contract terms, or a planned technology refresh should be included.

7. After sales support

7.1. Networking consultancy

Networking can be a complicated subject. CGI has network consultancy practice that can offer tailored network assessments, consulting on technical roadmaps as well as designing, configuring, and maintaining services. CGI specialists are certified by vendors including Cisco, Fortinet and Checkpoint.

Examples of areas for consultancy:

- Audit and Inventory Management.
- Design core, edge and cloud network solutions.
- Transition from data centre to cloud / moving toward software-defined networks / adopting ZTNA.
- Configuration, training and knowledge transfer.
- Assessment and optimisation to improve performance and user experience.
- Security / network segmentation / firewall reviews.

This service is typically provided on a time and materials basis, although a fixed price may be agreed depending on the defined scope and specification.

7.2. Service Requests

CGI and the client will jointly agree a service request catalogue, typically comprising simple and complex changes with associated process, SLAs and where applicable, any commercial considerations.

7.3. Driving Competitive Advantage and Innovation

To stay at the forefront of your industry, CGI will support you with aligning the network roadmap to meet short-term and long-term goals, prioritising projects based on business goals. Encouraging innovation through the ability to develop new services and increase automation without disrupting the rest of the business.

Most importantly, our people and our partners strive to support our clients to succeed. Through collaborating with our own specialists, our dedicated and trusted vendor experts and client stakeholders we can ensure a network that continues to support long term innovation.

7.4. Continual Service Improvement

Continuous Service Improvement (CSI) is embedded in CGI's Client Partnership Management Framework (CPMF) and underpins our services. CPMF includes defined processes and ways of working to continually improve the services that we deliver.

Our Service Model is underpinned by our ITIL 'good practice' Service Management Processes enabling us to align with your needs and embed CSI in our relationship. We also use traditional methods to deliver CSI including analysing key data inputs from tooling, undertaking trend and Root Cause Analysis, and leveraging end user feedback to identify opportunities to improve the end user experience.

8. Technical requirements

8.1. Connectivity

To manage and support your network environment, CGI uses secure connectivity methods such as VPN tunnels and, where required, dedicated private links. We will work closely with you to agree appropriate remote access configurations and determine where connections should terminate within your infrastructure.

Our CGI technical staff follow strictly controlled, audited access procedures when connecting to client environments, always ensuring security and compliance.

In cases where a dedicated connection or increased bandwidth is required to meet specific project needs or performance requirements, this may be provided at an additional annual cost and reviewed regularly to ensure suitability.

8.2. Hosting Services

When CGI provides managed network services within a client's own facilities or a third-party hosting environment, it is essential that the necessary infrastructure is available and maintained to support service delivery. The following components are required and should be provided by the client, their hosting provider or we can provide these services for you:

- Racking and floor space
- Structured building wiring
- Environmental provision (temperature and humidity control)
- Air-conditioning
- Uninterruptible Power Supplies (UPS)
- Access control to hosted environments.

These elements ensure a stable and secure foundation for the network infrastructure managed by CGI. We work collaboratively with clients to assess readiness and support the transition into a managed service model.

Where required, CGI can also provide fully managed hosting from our secure UK data centres, offering a complete end-to-end service that includes all the above components, monitored and maintained by CGI.

9. Outage and maintenance management

CGI will work collaboratively with the client to agree a schedule for routine operational patching and software upgrades, managed through the agreed Operational Change Management process. This schedule will cover all devices that form part of the Managed Network Service.

As part of our service, CGI proactively reviews vendor-issued updates to identify security vulnerabilities. We assess each update's relevance and risk to the client's environment and apply appropriate patches in alignment with the client's security policies and standards ensuring both protection and continuity.

10. Security

10.1. Information Assurance

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

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

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

Our accreditations include:

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

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

Information Principles for the UK Public Sector supported and documented

CGI recognises the UK Public Sector information principles which are fundamental to the efficient and effective delivery of public services. Where we store and manage government information in our G-Cloud services, we aim to ensure that it is appropriately protected and available to exploit. Through this, we aim to maintain and, depending on the service purchased, enhance the quality of the information stored in a standard manner that enables its re-use. Where the selected services require it, we would engage, both to support the buyer in the publication of public information and to support them in the access of information by citizens and business.

Government ICT Strategy and Greening Government ICT Strategy supported and documented

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

11. Service Pricing and Terms and Conditions

11.1. Pricing

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

11.2. Terms and Conditions

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

12. 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.

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

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.

Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured.

On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

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

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

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

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

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

Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765

