



SD-Access

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	10
3.	Service Continuity	11
4.	Onboarding and Offboarding	11
5.	Service constraints	12
6.	Service levels	13
7.	After sales support	14
8.	Technical requirements	15
9.	Outage and maintenance management	16
10.	Hosting options and locations	16
11.	Security	16
12.	Service Pricing and Terms and Conditions	17
13.	Further information	17
PROPRIETARY AND CONFIDENTIAL		18

Service Definition Overview

Software-defined networks (SDN) provide the foundation for the modern enterprise, establishing the underlying infrastructure to develop a secure, operationally efficient network which can be tailored to your business operation.

CGI's Software-Defined Access (SD-Access) solution, built on Cisco technology, offers a secure, policy-driven approach to managing wired and wireless network access. By replacing traditional network segmentation with identity-based, zero-trust access controls, SD-Access simplifies operations while enhancing visibility, flexibility, and security.

Our comprehensive service covers the full lifecycle—from network surveys and solution design to deployment and 24/7 UK-based support. With a centrally managed, scalable SD-Access fabric, CGI empowers your organisation with intelligent, adaptive connectivity that improves performance, supports innovation, and aligns with your evolving business priorities.

Features

- Centrally controlled, policy-driven network architecture spanning wired and wireless networks.
- Identity-based segmentation and access policies.
- Zero-Trust Network Access (ZTNA) and dynamic automation of access controls.
- Advanced performance analytics and application-level visibility.
- Zero-touch deployment of switches and wireless access points.
- Location-based wireless network analytics.
- Scalable architecture with AI-enabled self-healing and guided remediation.
- Fully managed network surveys, project managed hardware rollout, and configuration.

Benefits

- Improved user experience – Reliable connectivity and seamless access across your locations.
- Reduced complexity – Policy-driven automation simplifying network operations and reducing service impacting errors.
- Strengthened security – ZTNA and access segmentation enhancing protection and securing your data.
- Lower costs – Operational efficiency through centralised control and AI-based remediation.
- Faster innovation – Streamlined deployment and flexible architecture enabling change at pace.
- 24/7 UK-based support – Comprehensive coverage from CGI's Digital Command Centre.

Why CGI?

An SD-Access 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

CGI provides secure and reliable SDN technology to support your organisations ambitions and offer the potential to transform the day-to-day experience for customers and your employees.

Modern networks have become increasingly complex to manage. There are now a greater number of devices connected to LAN networks than ever before, the majority of which have a requirement for internet access.

This creates challenges for network designers and admins to identify what is connected to the network, why it is connected and what its access requirements are. As such, creating suitable network segments to segregate devices and user groups has become time consuming and prone to errors, and with that, come service challenges, cost, and potential security incidents.

To overcome these challenges, vendors have developed the concept of software defined network access.

In software-defined networking, the focus shifts from traditional networking to firstly identifying what is connecting, who is connecting and why is it connecting – what is the business intent of the connected device or user? Secondly, dynamically applying network configuration and policy based on business intent of that connecting device or user.

In large enterprise networks, software-defined access is now the only feasible approach to developing a new network. The alternative, traditional approach, becomes incredibly time consuming, inflexible to change and increasingly insecure.

1.1. Cisco SD-Access Solution

CGI utilises Cisco SD-Access technology to provide SDN solutions to public sector organisations. Cisco have the proven capability in developing solutions that can be designed and tailored specific to client environments, with direct benefits to your business needs, based on experience gained from previous deployments at enterprises around the world.

CGI has direct experience of designing campus networks to deliver operational efficiencies, continuous innovation, improved sustainability, and measured user experience.

We will manage, maintain, and monitor your SD-Access service from our Digital Command Centre (DCC) in Bridgend, offering 24x7 1st, 2nd, and 3rd line support, backed by full ITIL aligned service management model. Optionally, we can provide service desk, Security Operation Centre (SOC), and integration into IT Service Management platforms such as ServiceNow.

An SD-Access network is comprised of several components to manage access, define policy, and orchestrate the wider network.

The key components in a Cisco SD-Access are as follows:

Component	Type	Purpose
Wireless Access Points (WAPs)	Hardware	WAPs will provide the connection point for wirelessly enabled devices to access the network. WAPs will be located across your sites. CGI will assess the necessary WAP density to provide the required cross-site coverage.
Fabric Edge Switches	Hardware	Edge switches provide the bridge between the wireless network and the wired network, enabling wireless and wired devices access to your resources, cloud hosted apps and the Internet. Edge switches will be located across your buildings in comms rooms and wiring closets.
Fabric Core Switch	Hardware	The core switches provide an aggregation point for edge switches to connect back to central points within a campus building. The core switch also terminates wide area network (WAN) connections to allow

Component	Type	Purpose
		communication between users and devices in different campus buildings and data centres where applications are hosted, and internet gateways reside. Core switches will be in each of the main campus sites.
Catalyst Centre	Hardware or Virtual Appliances	Cisco Catalyst Centre controls the wireless network, edge, and core switches to provide a policy-driven network. Catalyst Centre is the dashboard through which the network is managed allowing administrators to configure the network without having to login on to individual switches. Catalyst Centre servers will typically be hosted in the client data centres or alternatively in the public cloud.
Identity Services Engine (ISE)	Hardware or Virtual Appliances	The ISE solution comprises several servers which allow network access to users and devices. ISE interfaces with the client's user directory, the edge switches, and the central firewalls to ensure the network is securely segmented based on user or device type and their business needs. The ISE servers will be hosted in the in the client data centres.
Wireless LAN Controller (WLC)	Hardware	The WLC enables central control and administration of the client's wireless access points and the distinct wireless networks through which users and devices can connect. The WLCs will be hosted in the in the client data centres.

Table 1 - SD-Access network component description

1.2. SD-Access - The CGI Approach

CGI's SD-Access solution is designed to provide you with a modern, software-defined network services platform on which to move forward with your strategic objectives and better prepare the network to underpin and meet the needs of the business.

Our goal is to evolve your network from a manual or semi-automated network to an intent-based solution ensuring the network directly supports your business goals. Moving to a software-defined network requires careful consideration and planning. We will work with you to undertake a phased approach to migration using lessons learned from other clients we have supported on this journey.

1.2.1. Supplier Solution - Project Initiation

CGI will create and agree with the client a Project Initiation Document (PID).

Both parties will define and agree the delivery acceptance criteria in the PID.

CGI will also create and maintain through the life of the project an Implementation Plan, which will include a detailed schedule of the project activities, inter-dependencies, timescales, and milestones. The Implementation Plan shall be a living document and regularly reviewed and updated throughout the life of the project.

1.2.2. Supplier Solution - Design and Engineering

CGI will assign a technical architect to work in partnership with the client. The architect will develop the SD-Access solution design following industry best practices.

CGI will deliver design and engineering services including network design, planning, scheduling, and integration required to migrate client services from the current network to a new network described in a High-Level Design (HLD).

CGI will provide and maintain new network system architectural specifications and topologies for all network services in scope.

During transition from the current network to the new network, CGI will review technical and procedural documentation, to ensure it remains current and accurate. Documentation will be updated to reflect the scope for extended network support.

CGI will support service integration and testing for all new or upgraded components based on documented requirements and outcomes. CGI will ensure that new or changing services meet agreed Test Success Criteria and Acceptance Criteria defined in the PID, before being moved into the production environment via the Acceptance into Service process.

1.2.3. Supplier Solution - Asset Acquisition

CGI will perform asset acquisition on behalf of the client. CGI will communicate expected lead times and delivery dates in line with an approved Implementation Plan. CGI will establish the required licensing, software, and warranty agreements on behalf of the client.

1.2.4. Supplier Solution - Integration and Testing

CGI will implement the SD-Access services by following an agreed standard Operational Change Management process.

CGI will ensure appropriate Testing for all new and upgraded SD-Access components as defined in an agreed Test Plan.

CGI will complete Acceptance into Service (AIS) checklists defined for the solution deliverables. AIS checklists will be written prior to change, ensuring that project engineers and network services team have agreed criteria prior to handover into service.

1.2.5. Supplier Solution - Training and Handover

CGI will define the required training and documentation handover for client staff. The format of training will include access to online training material provided by the network equipment vendor.

Where required, CGI will provide access to the network central service platforms, such as Catalyst Centre and ISE.

1.2.6. Supplier Solution - Site Surveys

CGI will perform desktop surveys using existing client network inventories. Where required, we will engage a third-party to support on-site cabinet and wireless network surveys.

1.3. Solution Deliverables

The following tables outline the CGI's approach for the design, deployment and support of SD-Access encompassing Core Network, LAN and Wi-Fi and Network Segregation. CGI shall deliver the programme as set out in the in the Project Initiation, Network Design and Network Deployment tables below.

1.3.1. Project Initiation

No.	Project Initiation Scope	Description of Supplier implementation approach
1.1	Project Initiation	- Hold Project kick-off meetings. - Agree timebound requirements for support from client SME's. - Agree an Implementation Plan and Project Schedule - Complete a Project Initiation Document

Table 2 - Project initiation outline

1.3.2. Network Design

No.	Core Network Scope	Description of Supplier implementation approach
3.1	Core Network Architecture	CGI will design the core network services encompassing network controllers, the fabric topology, network access control mechanisms and integration of the network with perimeter security services.
3.2	Site Discovery and Surveys	Complete site assessments, cabinet reviews and wireless surveys to ensure deployment is informed by real-world conditions.
3.3	LAN and Wi-Fi Design	CGI will produce site specific low-level designs for LAN and Wi-Fi deployments, supported by migration planning and testing methodology.
3.4	Network Segmentation	Define and implement macro and micro-segmentation policies across virtual networks to align with business requirements.
3.5	Hardware Deployment	CGI will manage the logistics of hardware delivery, staging and deployment ensuring alignment with project timelines.

Table 3 – Network Design approach

1.3.3. Network Deployment

No.	Core Network Scope	Description of Supplier implementation approach
3.1	Installation and Migration	CGI will perform phased installation and migration of switches, WAPs, and supporting infrastructure, working closely with client teams to minimise disruption. We will closely coordinate the network connectivity between current and new network infrastructure to ensure continuity of network access and services throughout the transition period.
3.2	Testing and Acceptance	- All deployments will be validated through structured testing, with each stage formally signed off via our Acceptance into Service (AIS) process ensuring support teams are kept in the loop throughout. - CGI will complete and maintain low level designs and site diagrams whilst ensuring network management systems, ITSM and configuration management databases are always up to date.
3.3	Post-Migration Activities	CGI will manage the decommissioning of the retired network and associated clean-up of legacy network configuration. As an additional service, we will provide security validation, including accredited IT Health Checks. We can responsibly dispose of legacy hardware where required. All activities are completed under change control and working to agreed procedures.

Table 4 – Network Deployment approach

1.4. In-Life Support Services

A well-implemented network with ongoing support from CGI, will drive competitive advantage and foster innovation for your organisation, ensuring the delivery of high-quality services in the following ways:

- A software-defined network's key concept is that it is programmable, not a static entity into which users, devices, and services must fit. An SD-Access solution can be easily adapted to meet the needs of your business.
- The network will provide the visibility, control, and assurance to enable rapid change when needed and aid the understanding and resolution of real or perceived service and application challenges.

Cisco Catalyst Centre offers a wealth of insight into network performance and in-turn the capability to maintain ongoing enhancements, using the tools and analytical data to continue to be proactive in performance management and reporting.

CGI has the skills and experience to get the best out of your SD-Access network. The following tables list the features and reports which we will support as standard in this service. Additional features can be leveraged based on client requirements. Reporting can be tailored based on client requirements.

SDN capability is ever-expanding. CGI can support API integration between SD-Access and IT Service Management tools, IoT and building management platforms, end-user device applications and many more. API integration is not included as standard in our SD-Access service; however, we will engage with clients to meet their specific business needs.

Automation Features

Feature	Description
Network Discovery and Inventory	Automatically discover and map the physical topology. Store all cisco fabric components with the Cisco Catalyst database.
Network Design and Profile Management	Domain and building categorisation for network device configurations.
Network plug'n'play	Zero touch device provisioning
Software image management (SWIM)	Software auditing and update push
Network compliance, audit, and remediation	Device configuration audit and recommended remediation
Policy creation	User and device access policies for ZTNA

Table 4 - SD-Access automation features

Assurance Features

Feature	Description
Network and client health dashboards	Assurance dashboards to identify network device anomalies and issues with clients connecting
Thousand Eyes integration	Application performance analysis
AI network analytics	Intelligent issue detection and analysis
Global assurance event viewer	Event correlation and root cause analysis
PoE analytics	Analyse switch power consumption for supporting IoT and smart technology

Table 5 - SD-Access assurance features

1.5. Table of services

The service and volume driver table below defines the information required to cost up the solution and provide a bill of materials. The service and volume drivers described will be assessed as part of a pre-sales engagement to allow for a bill of materials and cost estimate to be completed.

Service	Volume Driver
SD-Access Controllers	No. of end points
Network Access Control appliances	No. of end points

Service	Volume Driver
Wireless LAN Controllers	No. of wireless access points
Core and Distribution Switches	No. of core locations, physical topology, number of access switches, and bandwidth
Access Switches	No. of buildings, wiring closets, and wired endpoints
Wireless Access Points	No. buildings, internal and external layout, number of users
Site Surveys	No. of buildings and wiring closets
Wireless heat map surveys	No. of buildings
Design and deployment	No. of buildings and end points
Monthly Support	No. of switches and wireless access points

Table 6 - SD-Access services and volume drivers

1.6. Monitoring and Reporting

The table below describes the standard reports and reporting period included under the CGI SD-Access service.

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

Table 7 - Monitoring and reporting periods

Additional and/or alternative reports may be generated by exception. However, additional charges may be incurred to set them up.

1.7. Third Party Management

The service includes liaison with third parties who are sub-contracted to provide services and/or maintenance on elements of the network. This liaison may include:

- 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

Backup of network device configurations is achieved through Cisco Catalyst Centre and set to an agreed schedule.

Restoration of network device configurations is achieved through Cisco Catalyst Centre through zero-touch provision.

Replacement devices can simply be plugged into the network and configured to communicate with Cisco Catalyst Centre to obtain device configuration.

Cisco Catalyst Centre can be installed as virtual appliances. The client is responsible for providing the infrastructure upon which virtual machines can be established. The client is responsible for providing associated storage for network backup files.

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 lodged 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.

Our SD-Access service is designed to be resilient. This is achieved by providing clustered high-availability core components including Catalyst Centre, ISE, WLC and Core Switching. The degree of resilience will be dependent on underlying infrastructure provided by the client, including power and WAN connectivity. CGI will support the client by recommending scenarios to facilitate disaster recovery tests.

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 bring 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 notice 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 therein 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. 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.

5.2. 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).

5.3. 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.

5.4. 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 remote access. On-site attendance is provided subject to business need.

CGI will provide an event monitoring service for the SD-Access solution as part of its overall Service Management responsibilities. CGI teams will monitor events generated through alerts from monitoring tools such as Zabbix and Cisco Catalyst Centre.

- Where 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.
- Where CGI is not providing WAN connectivity, SLAs will be subject to those in place from associated WAN providers.
- Service availability will be defined based on the specifics of a clients SD-Access solution and components therein.
- CGI shall collaborate with the client to investigate and seek root cause for any Problems with investigation being handled by CGI.

6.1. Asset Ownership, licensing, and warranty

Cisco subscriptions or Enterprise Licence Agreement entitles all Cisco equipment to software support and updates for elected term.

Network hardware and software acquired under this service, comes under the ownership of the client.

Software and subscriptions required for this service must remain licenced for the duration of the contract term.

Hardware failures can occur during the service lifetime. Components are typically subject to lifetime warranty. To ensure expedited replacement of any faulty equipment, SLAs will be backed by an appropriate spare holding, or a vendor support package acquired through CGI.

6.2. 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.

6.3. Call Priorities

Note: for hardware related incidents and problems, Standard Support resolution indicated in the table below can only be achievable if a back-to-back SLA is put in place with the hardware maintainer.

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 8 - Incident response times

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 withdraw 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 should be introduced into the contract terms, or a planned technology refresh should be included.

Variance from the above means that Standard Costs plus a premium will apply.

7. After sales support

7.1. Networking consultancy

Networking can be a complicated subject. CGI has network specialists that can advise on designing, configuring, and maintaining services. CGI specialists are certified by vendors such as Cisco, Fortinet, Checkpoint, and HPE Aruba.

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 is the golden thread that runs through 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 Requirements

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. Client Requirements

It is the client's responsibility to provide the following services to support the SD-Access service:

- Racking and floor space.
- Building wiring, unless contracted through CGI.
- Environmental provision.
- Air-conditioning.
- Uninterruptible Power Supplies.
- General power provision.
- Access control to client environments.

9. Outage and maintenance management

CGI and the client shall agree a schedule of routine operational patching and software upgrades managed via the Operational Change Management process covering all devices comprising the SD-Access 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. Hosting options and locations

CGI SD-Access solutions will be hosted at client locations, third-party data centres, or in the public cloud, as defined by the client.

CGI works with all major cloud providers (AWS, Oracle, Microsoft Azure, Crown Hosting, Azure Stack and on-premises datacentres).

11. Security

11.1. 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.

11.1.1. 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 would 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 positively both to support the buyer in the publication of public information and to support them in the access of information by citizens and business.

11.1.2. 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.

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.

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

