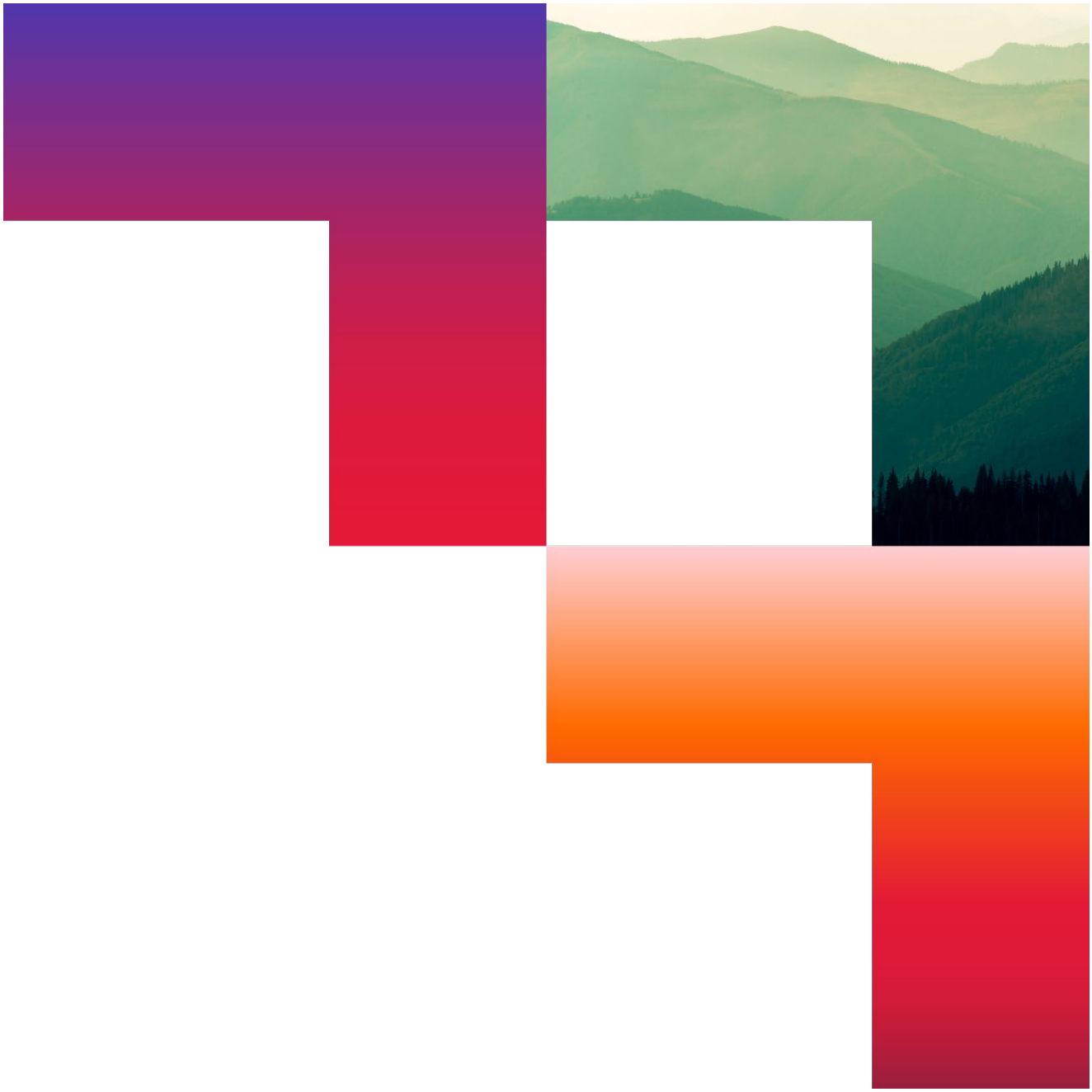


Network Health Check

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

CGI's Network Health Check provides an expert, independent assessment of an organisation's network estate, including LAN, WAN, Wi-Fi, telephony, data centre networking, and vulnerability posture. It identifies performance, configuration, security, and lifecycle risks and provides an actionable, prioritised remediation roadmap. The service supports organisations seeking to modernise ageing networks, prepare for cloud adoption, or improve resilience and security. The output includes heatmaps, tactical and strategic recommendations, and an Urgent–Important prioritisation matrix derived from detailed discovery and analysis.

Why CGI?

CGI brings deep expertise in UK public sector networking, cyber security and cloud-enabled transformation. Our client-proximity model ensures on-site engagement and contextual understanding; our domain experts are supported by global centres of excellence and specialist practices. We apply proven methodologies, leverage vendor partnerships across Cisco, Palo Alto, Juniper, Fortinet and leading hyperscalers, and deliver consistent quality via our global delivery network. Our advisory services integrate with broader Digital Leadership, CIO Advisory, FinOps and cloud readiness services, providing buyers with end-to-end capability and a consistent transformation approach.

1. Service Description

The CGI Network Health Check is a consultancy-based assessment of network health, risks and readiness. It uses a People – Process – Technology methodology, producing structured findings, heatmaps and a prioritised improvement roadmap.

1.1. People

Stakeholder interviews to understand roles, responsibilities, pain points, operational constraints and network management practices.

Capability and skills observations to identify gaps in tooling familiarity, operational process adherence, and network governance.

1.2. Process

Review of network configuration management, monitoring, incident/problem processes, change control, security processes, backup and patching approaches.

Assessment of alignment to organisational policies, industry good practice and operational dependencies (e.g., telephony, data centre, cloud).

1.3. Technology

Assessment components include (aligned with typical customer scope):

- **LAN** – core switching, data centre switching, firewalls (internal/external/DMZ), distributed switches.
- **WAN** – topology, link utilisation, resilience, routing protocols.
- **Wi-Fi** – coverage, authentication, security model, performance.
- **Telephony** – PBX, IP telephony, QoS and network readiness.
- **Data Centre Environment** – cabling, rack management, cooling, lifecycle and engineering considerations.
- **Vulnerability Assessment** – automated host, network and firewall scanning; authenticated scanning where permitted; analysis of missing patches, outdated software and insecure configurations.

1.4. Approach

The structured approach includes mobilisation, stakeholder interviews, discovery across each domain, vulnerability scanning, analysis, and a consolidated report:

- Immediate checkpoint – verbal alert if critical issues or indicators of breach are identified.
- Weekly checkpoint – progress and issues summary.
- Draft report within ten working days of discovery completion.
- Final report within ten working days after feedback.

1.5. Deliverables

- Executive summary and strategic challenges.
- Detailed findings per scope area.
- Tactical and strategic recommendations.
- Design, configuration, status and performance heatmaps.
- Urgency vs Importance matrix.
- High-level business case support for investment decisions.

This is a consultancy service. No hosting, operations, or managed service activities are provided.

2. Onboarding and Offboarding

2.1. Onboarding

Kick-off meeting and agreement of scope, success criteria and working arrangements.

Access enablement: read-only credentials, network diagrams, device inventories, monitoring tools, floorplans (where relevant).

Confirmation of scanning windows for vulnerability assessment.

Stakeholder scheduling and interview planning.

2.2. Offboarding

Delivery of all artefacts, reports and outputs.

Knowledge-transfer playback session.

Removal of all access credentials by the buyer.

Formal service closure.

3. Service constraints

Consultancy only – no operational run, no 24 by 7 support.

Read-only access may limit depth of findings.

All scanning will be scheduled to avoid service disruption.

Scope limited to buyer-owned or buyer-authorised network segments.

Timelines dependent on buyer SME availability and documentation quality.

4. Service levels

Response to queries during delivery: within two working days.

Draft report issued within ten working days of discovery completion.

Final report issued within ten working days of buyer feedback.

Checkpoints as defined in service description.

5. After sales support

A post-engagement Q&A window of up to ten working days.

Optional playback session for stakeholders.

Support in planning next-step remediation or integration with related CGI advisory services.

6. Technical requirements

To execute the assessment effectively, the buyer should provide:

- Read-only access to network devices, configurations and monitoring tools (e.g. SNMP, SolarWinds, WhatsUp).
- Relevant documentation: network diagrams, inventory, previous audits/health checks, incident/problem logs.
- Authorised vulnerability assessment scanning allowance.

- Named SMEs for LAN, WAN, Wi-Fi, telephony and security domains.

7. Security

CGI personnel are BPSS-cleared as standard; higher levels available if required.

Access is least-privilege, time-bound, and monitored.

All data stored within CGI systems is encrypted at rest and in transit.

Data retention follows CGI policy and buyer agreement; all artefacts can be securely deleted on request.

Scanning activity follows safe-practice procedures to avoid network impact.

8. Service Pricing and Terms and Conditions

8.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

8.2. Terms and Conditions

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

9. 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:

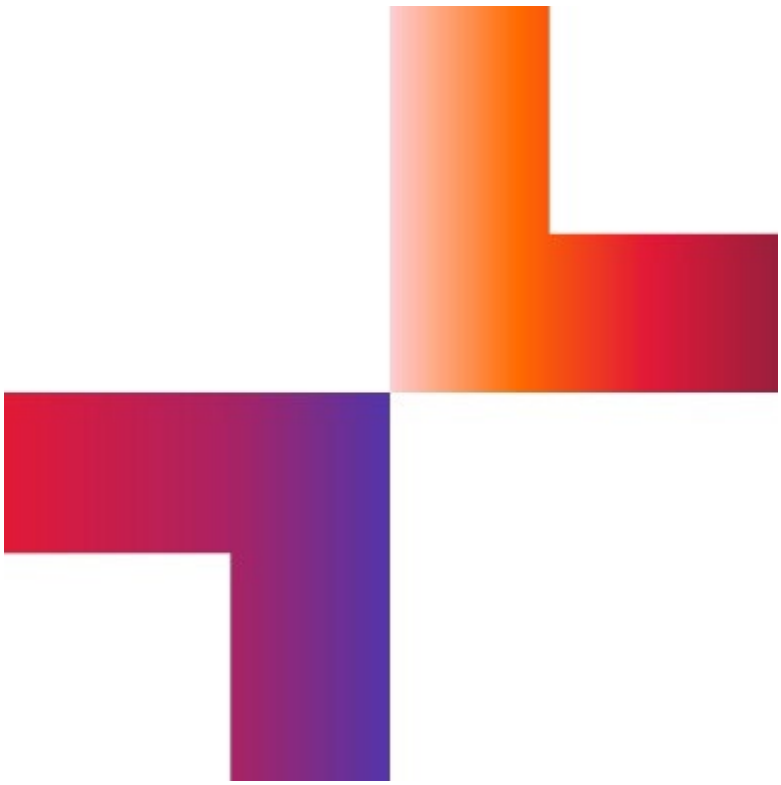
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk