



Infrastructure Health Check

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
1.1.	Potential health check scope areas	4
1.2.	People	4
1.3.	Process	4
1.4.	Technology	4
1.5.	Deliverables	4
2.	Data backup and restore	4
3.	Service Continuity	5
4.	Onboarding and Offboarding	5
4.1.	Onboarding	5
4.2.	Offboarding	5
5.	Service constraints	5
6.	Service levels	5
7.	After sales support	5
8.	Technical requirements	5
9.	Outage and maintenance management	6
10.	Hosting options and locations	6
11.	Security	6
12.	Service Pricing and Terms and Conditions	6
12.1.	Pricing	6
12.2.	Terms and Conditions	6
13.	Further information	6
PROPRIETARY AND CONFIDENTIAL		7

Service Definition overview

CGI's Infrastructure Health Check is a structured consultancy engagement assessing the health, risks, and readiness of an organisation's IT infrastructure, covering server, network, storage, backup, database, data centre, and vulnerability posture. The service identifies design weaknesses, lifecycle risks, configuration gaps, capacity issues, and security vulnerabilities, providing prioritised recommendations that support tactical remediation and strategic transformation. Outputs include heatmaps, urgency importance matrices, and business-case inputs to inform investment planning. Delivered across People – Process – Technology, the service is cloud-agnostic and suitable for hybrid and multi-cloud estates.

Why CGI?

CGI brings deep public-sector experience, a client-proximity model, accredited multi-cloud expertise (AWS, Azure, OCI), and a global delivery network. Our consultants combine domain knowledge across critical national infrastructure, cyber security and cloud operations with proven methodologies and repeatable accelerators. We provide clear, evidence-based insight, supporting buyers to optimise cost, resilience, and performance while aligning to organisational strategy and DDAT operating models.

1. Service Description

This consultancy service provides an independent assessment of the current-state IT estate to highlight risks, vulnerabilities, and opportunities for optimisation. Typical drivers include technical debt, security exposure, performance issues, capacity challenges, ageing infrastructure, and preparation for cloud modernisation.

1.1. Potential health check scope areas

- **Servers:** OS/hypervisor versions, patch status, lifecycle, utilisation.
- **Network:** LAN/WAN design, firewalls, supportability, capacity.
- **Storage and Backup:** firmware, regimes, lifecycle, utilisation.
- **Database & Applications:** versions, support status, configuration, dependencies.
- **Data Centre:** cabling, rack management, cooling, engineering, fitness for purpose.
- **Vulnerability Assessment:** host/network/firewall scanning, prioritised findings, mitigation guidance.

1.2. People

- Stakeholder interviews, roles and responsibilities mapping.
- Review of skills, operational practices, and ownership models.
- Identification of gaps affecting resilience, cost control, or operational maturity.

1.3. Process

- Assessment of incident, change, problem and configuration processes.
- Evaluation of backup regimes, patching processes, security monitoring, and network management workflows.
- Alignment checks against cloud-ready operating models and governance practices.

1.4. Technology

- Read-only discovery across infrastructure components using client-approved access.
- Automated data collection for configuration, capacity, performance, and security posture.
- Vulnerability scanning with expert triage to remove false positives.
- Production of technology heatmaps covering design/configuration, lifecycle status, performance, roadmap risks.

1.5. Deliverables

- Immediate verbal checkpoint for critical issues (e.g., breach indicators).
- Weekly progress updates.
- Draft report within ten working days of completing discovery; final report within ten working days of feedback.
- Strategic and tactical recommendations, RAG heatmaps, Urgent vs Important matrix, and business-case inputs.

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

2. Data backup and restore

Not applicable – consultancy service. We do not host or operate buyer systems. We assess the buyer's backup and restore posture and report any gaps.

3. Service Continuity

Consultancy delivery only. We provide resource substitution and rescheduling to maintain continuity. Buyer platform continuity and DR remain the buyer's responsibility.

4. Onboarding and Offboarding

4.1. Onboarding

- Kick-off and access enablement.
- Agreement of scope, stakeholders, success criteria, and discovery schedule.
- Secure provisioning of read-only access and documentation.
- Confirmation of communication channels and escalation paths.

4.2. Offboarding

- Handover of all artefacts and reports.
- Playback session to walk through findings and recommendations.
- Removal of CGI access credentials.
- Optional follow-on advisory or remediation consultancy.

5. Service constraints

- Consultancy only – no operational management of services.
- Read-only access is required for discovery (or a client proxy).
- Automated scanning scheduled with the buyer to avoid disruption.
- Scope limited to buyer-owned or buyer-authorised environments.
- Buyer SMEs required for timely workshops and evidence gathering.
- Change of scope via agreed change control.

6. Service levels

- Response to buyer queries: within 1 working day.
- Weekly checkpoint updates.
- Draft report delivery: within 10 working days post-discovery.
- Final report: within 10 working days of receiving feedback.

7. After sales support

- Up to one post-engagement playback session.
- Clarifications on findings for 30 days after final report submission.
- Optional follow-on services such as Well-Architected Assessment, Cloud Readiness, Cloud Operating Model, or FinOps advisory.

8. Technical requirements

- Read-only access to infrastructure within scope.
- Access to monitoring tooling (e.g., hypervisors, SNMP tools, SolarWinds, WhatsUp Gold).
- Access to inventory lists, diagrams, audit reports.
- Named technical SMEs available for interviews.

- Buyer-provided VPN or secure remote access route.

9. Outage and maintenance management

Not applicable - consultancy service. We do not run a live service. Any automated discovery is scheduled with the buyer to avoid impact.

10. Hosting options and locations

Not applicable - no hosting is provided. Work is performed within the buyer's cloud environments. Delivery is UK based by default.

11. Security

- CGI personnel are BPSS-cleared as standard; higher levels available if required.
- Access is least-privilege, time-bound, and monitored.
- All data remains in the buyer's environment unless expressly agreed for offline analysis.
- Artefacts stored securely within CGI collaboration environments and deleted in line with buyer retention instructions.
- Encryption used for all data transfer and report delivery.

12. Service Pricing and Terms and Conditions

12.1. Pricing

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

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

