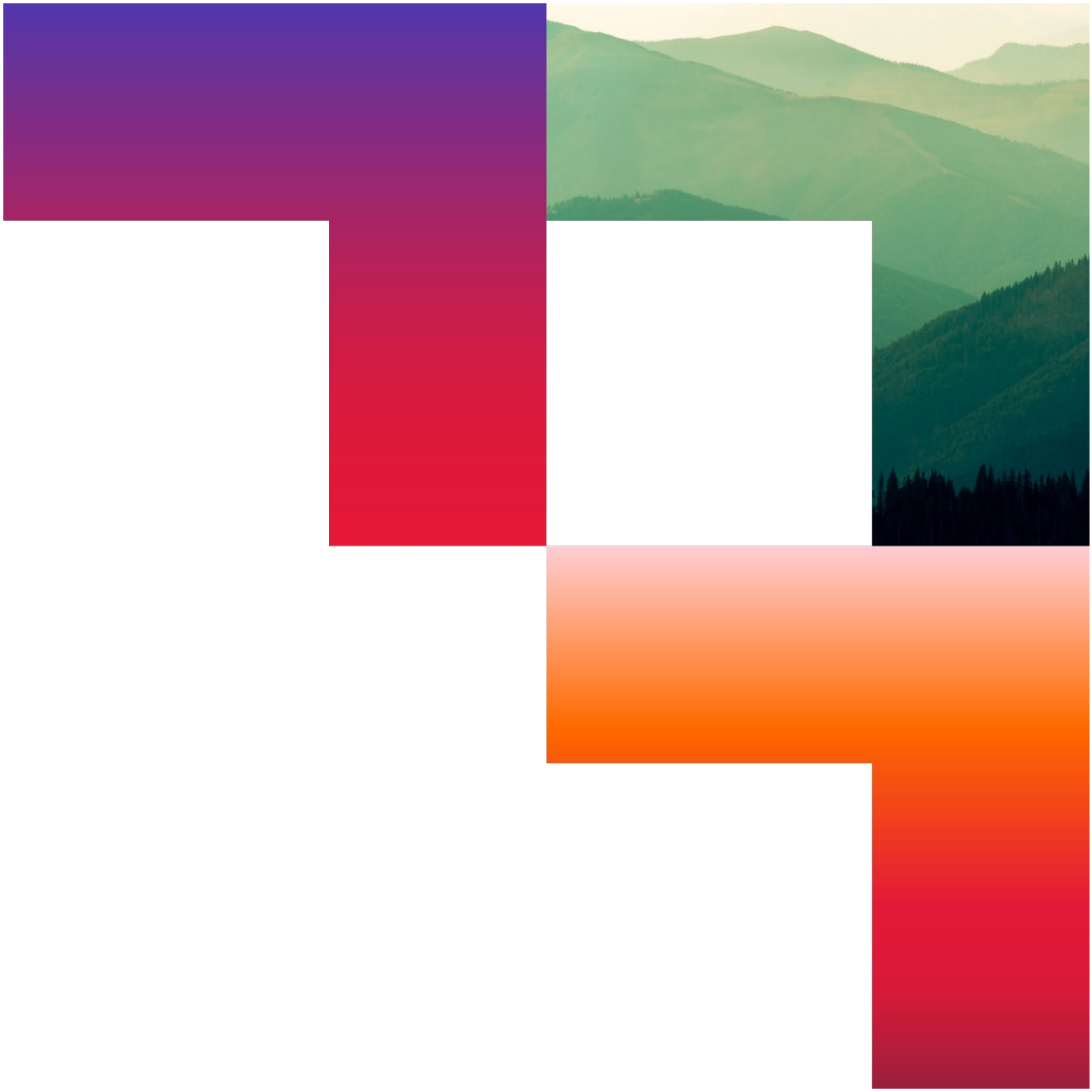


Cloud Health Check and Intervention (AWS, Azure and OCI)

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition Overview

CGI's Cloud Health Check and Intervention is a short, targeted consultancy service that diagnoses and stabilises existing cloud estates on AWS, Azure and Oracle Cloud Infrastructure (OCI). We rapidly assess people, process and technology to surface risks, cost drivers, performance bottlenecks and governance gaps, then prioritise remediation options that buyers can deliver themselves or with CGI support. Outcomes typically include a quantified risk register, a cost optimisation plan, a remediation backlog, and a concise executive summary for senior decision makers. The service is advisory and non-intrusive by default, with optional guided intervention sprints where urgent fixes are required. Work is performed within the buyer's environments and in full alignment with UK public sector standards and GDaD roles.

Why CGI?

CGI combines local, client-proximity delivery with deep domain expertise in UK Government and critical national infrastructure, backed by a global delivery network and multi-cloud partnerships (AWS, Microsoft, Oracle). We bring proven methods for cloud operating models, FinOps, DevOps and security engineering, and we tailor them to each buyer's policies and constraints. Our approach is outcome-led, measurable, and designed to be adopted by your teams, not to create supplier dependency.

1. Service Description

1.1. Scope and objectives (what this service does)

We assess live cloud estates that are experiencing acute issues (for example, security incidents or service instability) or organic challenges (for example, rapid spend growth, performance degradation, or governance drift). We provide a prioritised set of actionable findings and, where requested, deliver short intervention sprints to reduce the most material risks and costs.

1.2. Method (People - Process - Technology)

- People - Interview stakeholders across Digital, Security, Finance and Operations; assess roles, responsibilities and skills against GDaD role expectations; identify ownership gaps and handoff pain points.
- Process - Review change, incident, problem and release processes; evaluate governance (tagging, policy-as-code, approvals), FinOps cadence, incident playbooks, and compliance evidence paths.
- Technology - Inspect landing zones, identity and access management, network boundaries, logging and monitoring, backup posture, configuration baselines, performance and cost telemetry. Use native tools (for example, AWS/Azure/OCI Advisors, cost management), CIS and cloud well-architected checks, plus buyer-approved scanners.

1.3. Typical activities and deliverables

- Rapid discovery and evidence capture (read-only where possible).
- Security and compliance review - IAM hygiene, least privilege, encryption at rest/in transit, logging coverage, vulnerability and patch posture, alignment with buyer policies and applicable standards.
- Cost optimisation assessment - Rightsizing, scheduling, storage tiering, reservation/commitment management, waste elimination, tagging quality, showback/chargeback readiness.
- Performance and availability analysis - Application response baselines, latency hotspots, scaling and resilience patterns, DR readiness.
- Governance and management - Resource hygiene, automation guardrails, policy enforcement, change controls, SLA realism.
- Data management posture - Backup coverage and RPO/RTO feasibility checks, restore tests where requested, data lifecycle controls.

1.3.1. Findings and recommendations pack

- Executive summary (CIO/CISO/CFO-ready).
- Prioritised findings log with severity, impact, and owner.
- Remediation backlog (quick wins in 0–30 days; near-term 30–90; strategic >90).
- FinOps saving opportunities with quantified ranges and confidence rating.
- Target landing-zone or pattern improvements (reference architectures).
- Optional intervention sprint(s) to implement chosen remediations alongside buyer teams.

1.4. Example use cases

- Acute incident response triage after a breach or ransomware event to restore stability and close critical control gaps.
- Spend spike diagnosis where organic growth has outpaced FinOps maturity.
- Independent assurance ahead of major audits, go-lives or supplier transitions.
- Benefits (measurable, indicative ranges based on prior engagements).
- 10–25% cloud spend reduction from quick-win optimisation and governance improvements.
- 20–50% reduction in high-risk misconfigurations within the first intervention sprint.
- Improved service resilience (for example, verified backups and tested restores, clearer DR runbooks).
- Faster path to compliance evidence through structured findings and ownership.

1.5. Change control

The Statement of Work (SOW) fixes scope, assumptions, artefacts and access. Any material deviation (for example, additional accounts/subscriptions, extra regions, in-depth application tracing) is agreed via formal change control before work proceeds.

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. On-boarding

- Call-off confirmation and SOW sign-off.
- Access enablement (read-only cloud roles or proxy operators), NDA confirmations.
- Stakeholder and SME scheduling; artefact pack request (diagrams, policies, recent incidents, cost exports).
- Discovery workshops and tooling setup (buyer-approved only).

4.2. Off-boarding

- Playback of findings and agreement of remediation backlog.
- Handover of all artefacts (reports, evidence logs, IaC/code snippets from interventions).
- Access revocation confirmed by buyer; data retention clock starts per Security section.

5. Service Constraints

- Advisory and short-duration intervention only - no ongoing managed service or hosting.
- Standard working hours (UK business days) - no 24 by 7 operations.
- Scope limited to in-scope accounts/subscriptions/tenancies defined in the SOW.
- Buyer to provide timely SME access and read-only credentials or an approved proxy.
- Automated discovery and scanning only with buyer approval and in agreed windows.
- Remediation ownership remains with the buyer unless intervention sprints are explicitly contracted.

6. Service Levels

- Kick-off within 10 working days of order, subject to access and SME availability.
- Discovery complete within 5–10 working days for a typical 3–6 account/subscription scope.
- Draft report within 5 working days of discovery close; final report within 5 working days of playback.
- Query response within 2 working days during the engagement and the post-engagement support window.

7. After Sales Support

- Thirty-day Q&A window after final report (email or two scheduled clinics).

- One optional executive playback session (up to 90 minutes).
- Minor clarifications and re-runs of metrics where evidence was gathered by CGI during the engagement.

8. Technical Requirements

- Named buyer sponsor and single point of contact.
- Access: read-only cloud roles (or supervised console sessions) for AWS, Azure or OCI; access to ticketing, CMDB, CI/CD and monitoring where relevant.
- Artefacts: current high-level and low-level architectures, network/security diagrams, key policies and standards, last three months of incident/problem records, and latest cost exports/tag dictionaries.
- For intervention sprints, change windows and approvals must be scheduled in advance; buyer to execute changes that require privileged elevation unless a proxy model is agreed.

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

- Access control - Principle of least privilege; named individual accounts; MFA enforced; access time-boxed to the engagement.
- Data handling - Evidence retained in encrypted repositories; no production data copied unless explicitly authorised and minimised; sensitive exports stored in buyer-approved locations.
- Encryption - All data in transit via TLS 1.2+; at rest using industry-standard encryption.
- Retention and deletion - Engagement artefacts retained for 90 days post-handover unless otherwise agreed, then securely deleted.
- Personnel - Consultants are UK-based by default and hold appropriate baseline personnel security screening; higher clearances can be provided on request.
- Buyer responsibilities - The buyer remains the data controller and is responsible for approving any scanning, data exports and change execution.

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

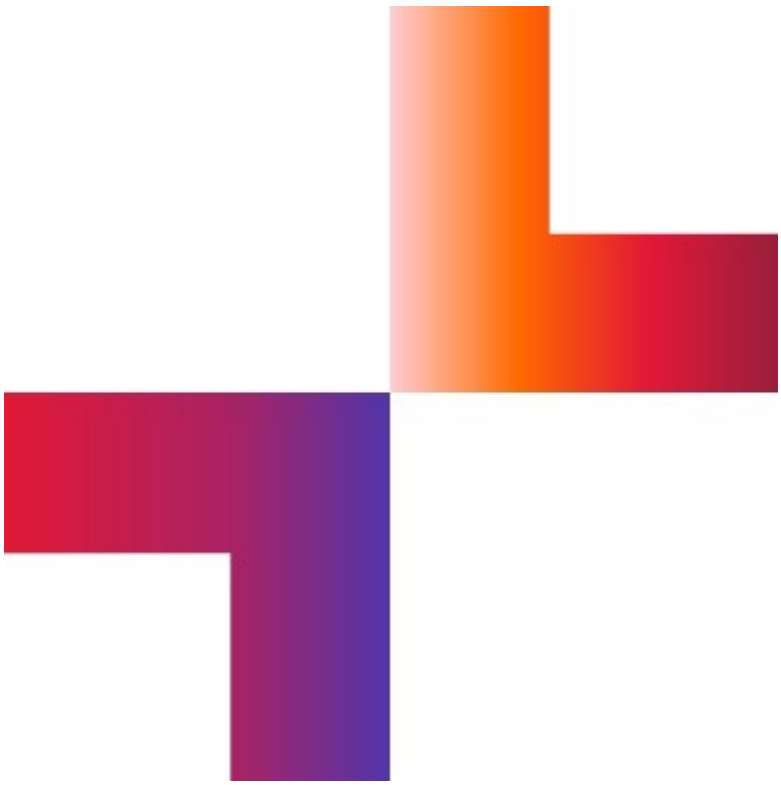
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk