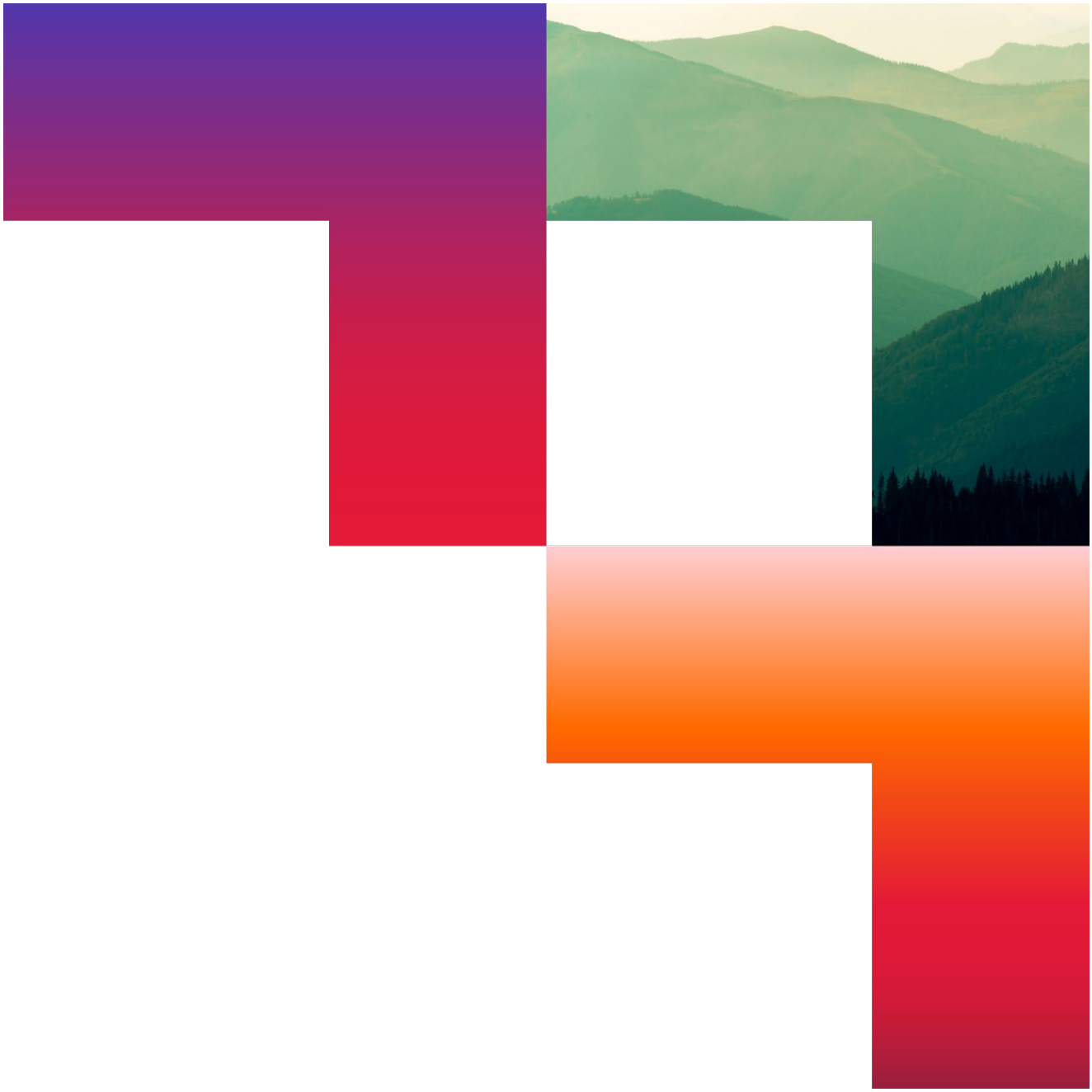


PCI DSS Health Check Service

Contracting body

30 Jan 2026

Issue 2.0

Table of contents

Service Definition overview

Organisations that are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) are now operating under the requirements of PCI DSS v4.0, which became the baseline standard following the transition period that commenced in April 2024. All new PCI DSS assessments are conducted against v4.0, and organisations previously certified to earlier versions are now expected to have completed their transition to the updated standard.

CGI has extensive experience supporting organisations through both the transition to PCI DSS v4.0 and full end-to-end implementations for those new to the standard. We can guide clients through gap analysis, remediation planning, control implementation, and preparation for formal assessment, leading to certification and attestation of compliance.

Organisations that are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) are now operating under the requirements of PCI DSS v4.0, which became the baseline standard following the transition period that commenced in April 2024. All new PCI DSS assessments are conducted against v4.0, and organisations previously certified to earlier versions are now expected to have completed their transition to the updated standard.

CGI are able to guide and support organisations to allow for clear identification of non-compliance elements and consequently help prioritise and implement security tasks to attain full compliance and applicable certification and attestation to the new v4.0 requirements.

Why CGI?

For over 40 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services. Our ‘PCI DSS Health Check Service’ builds on this solid background by amplifying our security management capabilities and dovetailing with our comprehensive suite of related Cyber Services.

Our experienced consultants work collaboratively with organisations to undertake a PCI DSS Health Check service, bringing to bear our lessons learned, knowledge and experience in overcoming the PCI DSS compliance hurdles. Our experience, combined with our PCI DSS Health Check methodology, structured questionnaires and compliance assessment tools, provide a consistent and successful outcome.

1. Service Description

The CGI PCI DSS Compliance Health Check service delivery and approach goals will include:

- Understand your business context - Help you clearly understand your PCI DSS compliance obligations and options to ensure no unnecessary compliance requirements are added.
- Understand your payment card scope - This will include identifying the full card data traffic flow that may also include boundaries by 3rd parties, their compliance requirements and additionally help you setup your own necessary due-diligence to ensure full payment card eco-system compliance.
- Assess your organisation against the v4.0 standard, either as a merchant reporting to your bank, or as a service provider.
- Support you where necessary to deploy PCI DSS compliant systems and if necessary to remove others e.g. obsolete software and hardware from scope through an assisted security improvement development programme.
- Utilise tried and tested PCI Security Standards Council Prioritised Approach and tooling.

Our PCIDSS Health Check Assessment Service activities will centre around standard gap-analysis activities such as:

- The relevant business processes and assets in relation to payment card activities.

Understanding of Card Handling processes and current status of compliance (if any).

- Facilitated workshops to confirm PCI DSS scope and determine whether self-assessment (SAQ) or a formal on-site assessment is required.
- Identification of control gaps and development of a prioritised remediation roadmap aligned to PCI DSS v4.0 requirements.

The PCI Security Standards Council Prioritised Milestone Approach shall be utilised as noted headline activities below:

Table 1 Prioritised Milestones

Milestone	Goals
1	Do not store sensitive authentication data and limit cardholder data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other account data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	Protect systems and networks and be prepared to respond to a system breach. This milestone targets controls for points of access to most compromises and the response processes.
3	Secure payment applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas are easy prey for compromising systems and obtaining access to cardholder data.
4	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning access to your network and cardholder data environment.
5	Protect stored cardholder data. For those organizations that have analysed their business processes and determined that they must store Primary Account Numbers, this milestone targets key protection mechanisms for the stored data.
6	Complete remaining compliance efforts, and ensure all controls are in place. This milestone completes PCI DSS requirements and finishes all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

As a result of the assessment and gap analysis, we develop and agree a detailed action plan, containing responsibilities and timescales, together with a summary of compensating controls where a requirement cannot be met.

The PCI DSS health check provides a report and presentation outlining our findings, gap analysis and key recommendations for improvements to achieve PCI DSS v4.0 compliance.

The comprehensive report includes:

- An executive summary.
- Gap analysis report to the PCI DSS v4.0 requirements.
- A summary of recommended actions.
- Use of the Prioritised Approach endorsed by the PCI Security Standards Council.

2. Data backup and restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the IA Backup / Restore policies as defined in ISO 27001; any information that has been processed as part of an engagement will be stored securely. Where applicable, this information can then be restored from an appropriate back-up, should the need arise.

3. Service Continuity

CGI will agree appropriate service continuity in accordance with any specific requirements, and any conditions that need to be met.

4. Onboarding and Offboarding

4.1. Onboarding

For Specialist Cloud Services, CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services, CGI understands the client's requirements and make on-boarding specific to these needs, using the experience, lessons learnt and methodology from many years of public sector transition experience, we can quickly align to client joiners, movers and leavers policies and ensure that we have appropriately cleared staff for every engagement.

4.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

4.2.1. Access to data upon exit

Deletion of any virtual machine image 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. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any computer or storage device or media that remains part of CGI's estate, with the exception of any data related to a data retention agreement between a client and CGI.

5. Service constraints

CGI will work with you to define and tailor the services to meet your specific requirements. During this definition period, detailed responsibilities will be agreed across the service delivery. Examples of common general constraints are listed below:

Share the existing internal sponsorship and governance for Information Assurance.

Assign or appoint a suitably skilled and empowered person to act as the receiving client.

Provide appropriate access to its policies, processes and standards for the Information Assurance service and other suppliers.

Provide timely information relating to its business plans, goals and projects.

As a main feature of any Service will necessitate an on-going dialogue with client representatives, the most important responsibility of the Contracting Body is to ensure the timely availability of individuals for fact-finding interviews.

6. Service levels

The overall accountability for the relationship with the client lies with CGI's Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

7. Hosting options and locations

CGI has a network of 21 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

8. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organization to protect information assets, technologies, facilities and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organizational measures are defined using a risk-based approach. This takes into account the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum security standard for all CGI offerings (including cloud based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to take into account specific requirements (risks, regulatory requirements, etc.)

these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client

9. Service Pricing and Terms and Conditions

9.1. Pricing

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

9.2. Terms and Conditions

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

10. 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 2.0 on behalf of CGI by the following authorised representative:

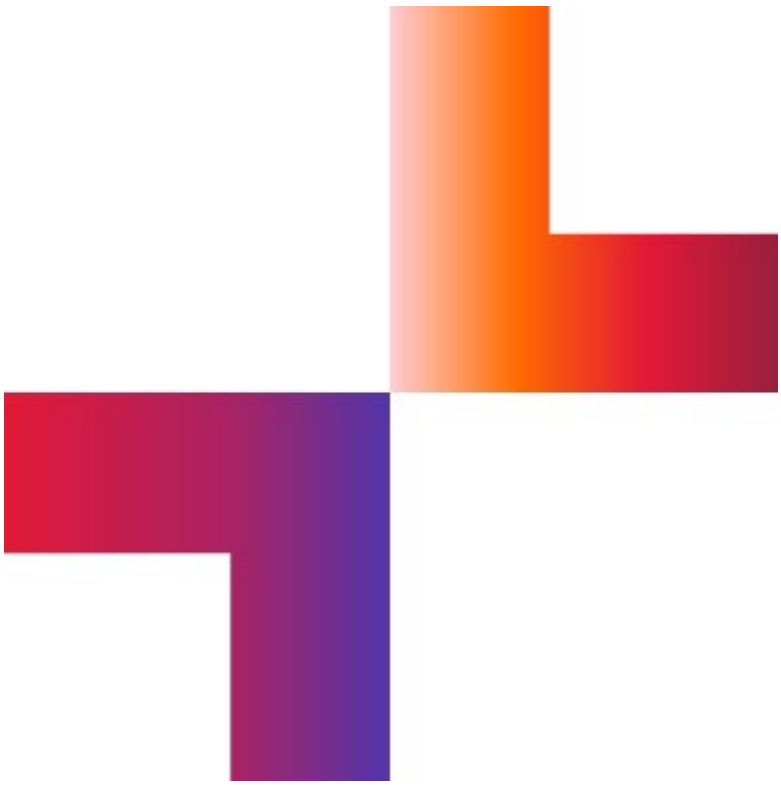
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk