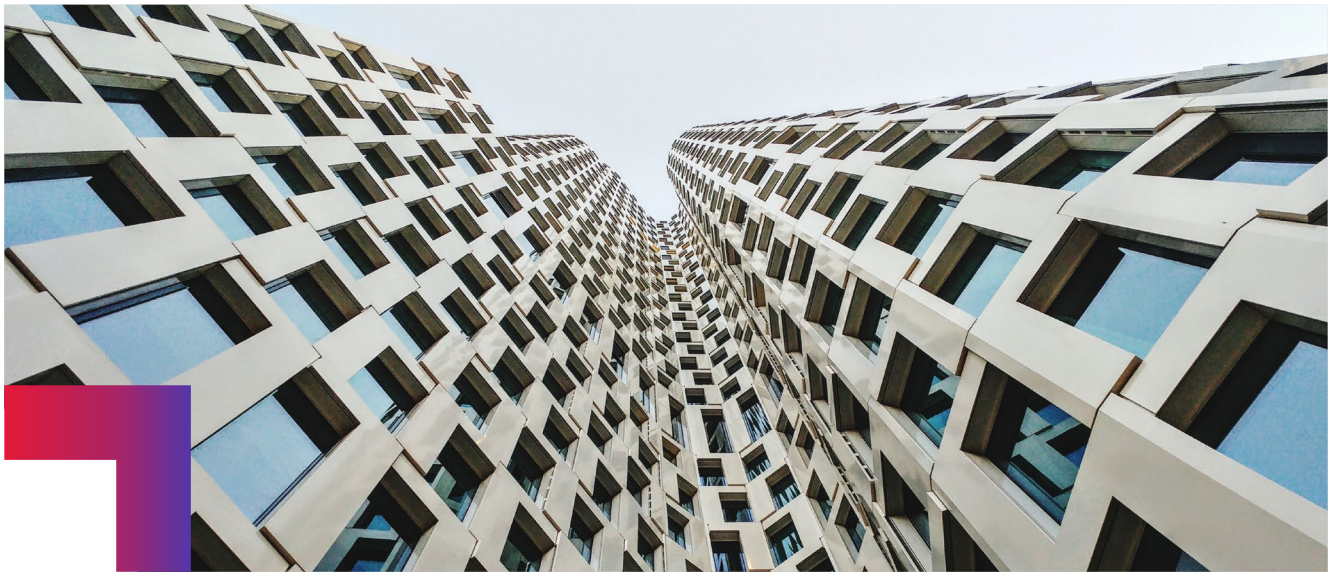
Payment Card Industry Data Security Standard

(PCI DSS) Compliance Readiness Service



CGI PCI DSS Compliance Readiness Service

Secure payments. Continuous compliance. Confident operations.

At CGI, we help organisations across the UK proactively navigate the evolving requirements of Payment Card Industry Data Security Standard (PCI DSS). Our PCI DSS Compliance Readiness Service equips you with a structured and collaborative pathway to validation, ensuring that compliance is not only achieved, but sustained, aligned with your operational goals and threat landscape.

Whether you are preparing for your first PCI DSS audit, managing changes with the latest version of the standard, or seeking ongoing assurance, CGI provides tailored guidance and practical support every step of the way.

Through our PCI DSS Compliance Readiness Service, CGI works with you to:

- Assess your current environment
- Identify compliance gaps through structured readiness activities
- Provide clear reporting and roadmap actions to meet current and emerging standards

We support PCI DSS compliance for both merchants and service providers, and where required, CGI can provide Approved Scanning Vendor (ASV) and Qualified Security Assessor (QSA) services through our trusted partner network, ensuring independent validation and confidence.

Why CGI?

With over 50 years of experience in securing critical government and commercial environments, CGI combines technical depth, risk understanding, and a pragmatic delivery approach to help organisations meet PCI DSS obligations without unnecessary overheads.

Our PCI DSS Compliance Readiness Service is delivered by seasoned cyber consultants and seamlessly integrated into CGI's broader Cyber Security Services, including governance, advisory, and technical support.

What sets us apart:

Expert guidance grounded in real-world experience and regulatory insight

A proven methodology including tailored scoping, gap analysis, and risk-aligned roadmaps

Focused support that adapts to your business context, data flows, and third-party involvement

Service description

The Payment Card Industry Data Security Standard (PCI DSS) is a critical requirement for any organisation processing cardholder data. The standard evolves frequently, and failing to comply exposes organisations to:

- Financial penalties
- Reputational harm
- Loss of access to payment platforms

CGI supports you across the entire compliance lifecycle, whether you are implementing PCI DSS for the first time or upgrading your controls for new regulatory demands. We help you:

- Clarify your scope and obligations
- Identify and remediate non-compliance elements
- Streamline compliance activities through risk-based prioritisation
- Support attestation through collaboration with QSA partners

Our readiness approach

CGI's PCI DSS Compliance Readiness Service includes the following stages:

1

Understand your business context

- Identify your specific PCI DSS obligations
- Avoid unnecessary compliance overhead by aligning strategy to real-world operations

2

Define payment card scope

- Map payment data flows, including third-party dependencies
- Support due diligence and vendor assurance to ensure ecosystem-wide compliance

3

Assess against the latest standard

- Apply gap analysis and maturity assessments across the standard
- Identify remediation and risk reduction opportunities
- Clarify whether formal QSA validation or self-certification is appropriate

4

Develop your security improvement programme

- Support de-scoping where possible (e.g. obsolete systems)
- Prioritise and implement technical and organisational controls
- Align with PCI Security Standards Council's Prioritised Approach and supporting tooling

Delivery activities include:

- Workshops to scope compliance effort and map out key assets, people, and processes
- Structured assessment of cardholder data environments and control maturity
- PCI DSS roadmap planning with milestones and success metrics
- Executive-level reporting to communicate current risks and strategy alignment
- Optional liaison with ASV/QSA partners for audit support or external validation

Why now?

The latest version of the standard v4.0.1 was released in June 2024 has introduced significant changes in expectations, further emphasising controls such as enhanced monitoring, and risk-driven validation. Don't wait for audit deadlines to act. Let CGI help you transform PCI compliance into a proactive pillar of your cyber strategy.

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 organisations 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.

Action plan and reporting

Following our gap analysis and collaborative assessment, CGI develops a detailed and actionable remediation plan. This includes:

- Clearly assigned roles and responsibilities
- Agreed timelines for remediation activities
- Identification of compensating controls where full compliance is not technically or commercially feasible

This ensures your organisation has a clear, realistic roadmap to achieving PCI DSS compliance, prioritised by risk, aligned to operations, and ready for board and auditor visibility.

Deliverables: Comprehensive readiness reporting

At the conclusion of our engagement, CGI delivers a PCI DSS Compliance Readiness Report and executive-level presentation that includes:

- **Executive Summary:** High-level findings, risks, and next steps tailored for senior stakeholders
- **Gap Analysis Report:** A structured review against the most recent PCI DSS requirements
- **Recommended Actions:** Prioritised activities across technology, process, and governance domains
- **Compensating Controls Summary:** Documented measures to reduce risk where full compliance is not immediately achievable
- **Prioritised Approach Alignment:** Use of the PCI Security Standards Council's Prioritised Approach to structure your remediation programme

Additionally, should your organisation require formal attestation, CGI can support this by engaging a Qualified Security Assessor (QSA) through our trusted partners, enabling a seamless transition from readiness to full Attestation of Compliance (AoC).

Ongoing support and integration

CGI also offers continued advisory and managed services to support:

- Ongoing control implementation and validation
- Transition planning to the latest version of the standard
- Integration with broader governance and cyber resilience strategies
- Managed compliance monitoring through CGI's SOC and cyber platforms

Our approach is not only about meeting the current standard, but building long-term, risk-informed PCI resilience as part of your overall security posture.

Compliance with confidence. Payments without compromise.

- Email cyber.enquiry.uk@cgi.com
- Visit cgi.com/uk/cyber-security

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.