Bridewell

Payment Card Industry Data Security Standard (PCI DSS) Services

Whether taking payments into your own bank accounts or enabling customers to process payments by providing services such as network connectivity or hosting, you are in scope of PCI DSS. Our range of pragmatic, fully consultative services can help you ensure a streamlined and efficient process for: defining your PCI DSS scope, applicable PCI DSS requirements, identifying de-scoping options, remediating deficiencies, formal assessment and ongoing support.

Common Challenges

PCI DSS Applicability Unknown – Confirming if, how, and why you are in scope of PCI DSS can be confusing but is imperative to identify how you interface with payments, your compliance reporting entities/ stakeholders, compliance reporting method(s) to be used, and any possible penalties / fines associated with being non-compliant.

Unknown Cardholder Data Environment – It can be difficult to know what people, processes, and technology form the scope of your cardholder data environment (CDE), especially when introducing new payment channels, following organic growth or completion of mergers and acquisitions.

Unknown Applicable PCI DSS Requirements – Once a CDE has been defined, it is often challenging to identify which PCI DSS requirements are applicable to the system components that comprise the CDE.

Lack Of In-House PCI DSS Expertise – Organisations often have an absence of subject matter expertise to support with navigating PCI DSS compliance reporting, maintaining compliance, and resolving other associated business or technical challenges.

How Bridewell Can Help

Demystifying Your Compliance Requirements – Performing a scoping exercise enables you to understand your PCI DSS compliance reporting requirements, your current CDE scope, applicable requirements, and any de-scoping options, allowing you to focus resources where required.

Understanding Your Current Compliance Posture – Validate your current level of compliance for DSS requirements to ensure that there are no hidden surprises during a formal assessment that could jeopardise your PCI DSS compliance.

Fully Consultative Assessments – Through careful planning and preparation, a structured approach to evidence collection and pragmatic methodologies for the management and remediation of any identified compliance challenges, Bridewell guarantees a streamlined and efficient assessment process.

Streamline Ongoing Compliance – Ongoing check-ins and compliance validation by a Qualified Security Assessor (QSA) between anniversaries provides assurance that activities are being completed in line with PCI DSS requirements, and any potential compliance challenges that could be introduced through routine activities, or project and change management processes.

Preparing for PCI DSS Compliance?

Discuss your cyber security goals or PCI DSS challenges with our experts.

Bridewell

1. Scoping Exercise

- Clear definition of your PCI DSS scope including the people, processes, and technology that form the CDE and applicable DSS requirements.
- Provision of de-scoping options (where possible) to reduce initial and ongoing compliance burden.
- Defined PCI DSS compliance reporting obligations and compliance reporting entities.

2. Gap Analysis

- Per-requirement validation of the implementation status for each applicable PCI DSS requirement.
- Thematic and per-requirement findings and supporting recommendations specifying required remedial activities.
- Prioritised remediation roadmap to support the most appropriate allocation of resource and funding.

3. Remediation Support

- Pragmatic and consultative expert guidance to ensure remediation efforts meet PCI DSS requirements.
- Leading conversations with internal and external stakeholders relating to remediation and de-scoping activities.
- Creation of collateral to demonstrate DSS requirements are embedded within the organisation.

4. Assessments

- Fully consultative end-to-end assessment approach ensuring all stakeholders are prepared and informed throughout.
- Actions Tracker overseen by a QSA to ensure all queries, evidence requests, and identified non-compliances are tracked, managed, and resolved.

5. Ongoing Compliance Management

- Proactive management of routine activities completed by a SME to aide in the identification and remediation of potential or actual compliance issues.
- PCI expertise included within change and project management processes to ensure compliance challenges are not unknowingly introduced.
- Stay abreast of the latest updates and developments from the PCI Security Standards Council.

6. Approved Scanning Vendor (ASV) Vulnerability Scanning

- Provided as a managed service where a QSA is responsible for scheduling scans and consulting with you to remediate any identified issues or on a licence-only basis.
- Leverage QSA expertise to confirm how to manage false positives, confirm the correct scanning scope, and how changes may potentially impact ASV scans.

7. Technical Testing and Assurance

- Scoping and completion of penetration tests / code reviews / ruleset reviews of:
  - Web Applications.
  - Mobile Applications.
  - APIs.
  - Internal/External Infrastructure.
  - Traditional Firewall Rulesets.
  - Azure Network Security Group (NSG).
  - AWS Security Groups.
- Segregation testing of network segments to validate controls are operating effectively to reduce the scope of PCI DSS.

Get in Touch

+44 (0)3303 110 940

hello@bridewell.com

bridewell.com