

Payment Card Industry Data Security Standard Does it affect you?



The issue

The Payment Card Industry Data Security Standard (PCI DSS) is designed to protect a cardholder's credit and debit card details from misuse and applies to any organisation that stores, processes and/or transmits cardholder data. The standard is universal and set by the major payment card brands e.g. Visa, MasterCard, American Express, JCB and Discover. Merchants and service providers who do not comply with the standard can be subject to fines, held responsible for reimbursing the client for any loss, or in some cases have their authorisation to accept payment cards withdrawn.

We were approached by a highly renowned UK based trade institute; which also has localised overseas representation. They were seeking support to gain a credible position statement in relation to their existing level of compliance with the PCI DSS to demonstrate to their acquiring bank how they would satisfy their timeframe expectations for formal compliance validation against the standard's requirements.

The solution

Our initial visit highlighted that the information given to our client by the bank was inconsistent with the standard. We helped our client seek clarification by providing them with a list of questions to present to the bank. This resulted in a clear instruction to the client and an extension on the timeline that the bank had originally set. It was important to take this step to have clarity and also protect the reputation of the client.

We were then engaged to assist our client in achieving their objectives which were:

- To discover and report on the level of their current compliance requirements based on their transaction level and PCI DSS reporting requirements.
- Provide recommendations for remedial actions that they could consider taking to pragmatically meet their bank's reporting, compliance and timescale requirements.

During the course of our work, we reviewed the IT network, infrastructure, processes and controls against the 12 key PCI DSS requirements and reported the results to our client in the form of a gap analysis, a percentage of current compliance against each PCI DSS requirement and full recommendations for remedial actions.



Remedial activity was prioritised using the PCI DSS scorecard; a generic gauge to focus activity to meet compliance effectively.

We delivered our findings directly to the Executive Finance Committee; such is the importance of the PCI DSS. At the meeting the Finance Director endorsed a remediation project to address the gaps against the standard and reduce the immediate risk to reputation through non-compliance. A project was initiated, budgeted and a key project team was appointed to ensure that the project was kept to a manageable size. Subsequent to our involvement, we continue to support our client, as required, in line with our ongoing commitment to move them closer to self-sufficiency.

See www.kscllp.co.uk

Contact us

City

Nick Brooks +44 (0)20 7566 4000
Janice Riches +44 (0)20 7566 3804

Sandra De Lord +44 (0)20 7566 3764

St Albans

Gordon Follows +44 (0)1727 896040