

Taking the credit

If you accept credit or debit card payments, you need to be aware of the Payment Card Industry's (PCI) Data Security Standard. This is intended to protect cardholders' credit and debit card accounts and transaction information. Co-developed and introduced by Visa and MasterCard in January 2004, the PCI

Standard was last revised in October 2010. It is the framework used in Visa's Cardholder Information Security Programme and MasterCard's Site Data Protection programme to measure and validate compliance. American Express subsequently adopted the standard for its Data Security Operating Policy programme as did Discover and JCB; so now the standard is universal across all major payment card brands.

A framework

The Standard addresses 12 key security areas, providing a consistent framework for securing and monitoring cardholder data. Those organisations who do not comply can be subject to severe sanctions ranging from fines up to and including revocation of privileges by the card brands.

PCI data security requirements apply to all merchants and service providers that store, process or transmit cardholder data. These security

requirements apply to all system components, network components, servers or applications included in, or connected to, the processing of cardholder data.

What must you do?

Any organisation which accepts credit and/or debit cards for payment *must* comply with the Data Security Standard. Further, that compliance must be validated on a regular basis. The actual validation requirements vary according to the number of card transactions processed annually. However, as a minimum, a quarterly external network vulnerability scan must be conducted by an accredited security firm.

Most organisations are also required to have an annual on-site security audit, although in some cases a self-assessment questionnaire may suffice. Kingston Smith Consulting will be happy to provide you with the requirements appropriate to your organisation at no charge.

The standard's requirements

The following 12 requirements are the foundation of the standard:



Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmissions of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Programme

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know

- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

Can we help?

Kingston Smith Consulting employs fully accredited Qualified Security Assessors whose expertise is annually re-examined. We work with an Authorised Scanning Vendor using trained and experienced professionals qualified to perform PCI data security assessments.

Our Technology Risk Management professionals approach each engagement with a “can-do” perspective gained from years of working in high-risk, high-stakes IT environments.

Kingston Smith Consulting is able to provide a range of solutions to protect your business. We are able to assess the current state of your compliance with the standard, and assist you in implementing cost-effective measures where appropriate to bring you into a state of compliance.

We can also combine this with the annual security audit where necessary, together with the quarterly network scans.

If you have further queries, please do not hesitate to contact Mark Child for more information.

Tel: +44 (0)20 7566 3731
Fax: +44 (0)20 7689 2475
Mobile: +44 (0)7515 107005
Email: mchild@kscllp.co.uk

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010 info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD