inspired **solutions**

PCI DSSv2 compliance

PCI DSSv2 applies to all organisations that store, process or transmit cardholder data. It covers technical and operational system components included in, or connected to, cardholder data.

PCI DSSv2 Compliance

If you are a merchant who accepts or processes payment cards, you have to comply with PCI DSSv2. As a security standard PCI drives and builds on your existing security best practice. To ensure you comply and remain PCI DSSv2 compliant, there are 12 steps that you need to follow:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

What can APSU do for you?

We can determine how PCI applies to your business and your validation requirements because we work in partnership with you and a Qualified Security Assessor (QSA) to ensure that the PCI DSSv2 requirements are clearly understood by each party.

Once these requirements are finalised we tailor the appropriate solution to your specific business needs. Our experienced team will then progress and implement the agreed solution to time and within budget. Finally, when the implementation phase is complete, APSU will administer and secure the environment to ensure you maximise uptime and maintain ongoing compliance.

As a security accredited and respected solutions provider, we have worked with various businesses to ensure they are compliant. Our capability covers new infrastructures and the development of your existing infrastructure and processes with regard to compliance. PCI DSSv2 is rarely a point solution and our role is to make the process as painless as possible for the stakeholders involved.

For businesses that are conversant with PCI DSSv2 and are working towards their compliance, we can assist you with specific solution components required to complete compliance.

How do we work?

- We gain a detailed understanding of your PCI requirements and asses how they apply to you, drawing on experience gained from multiple QSA engagements.
- We scope, design and size an appropriate solution working with you and the QSA. This ensures the QSA approves the approach and solution up front.
- We are experienced in PCI DSSv2 Compliance and can manage the relationship with the QSA to ensure you get the right solution for your business.
- We can investigate integration of your environment with your partners environments and applications.
- We provide a project management plan to achieve PCI DSSv2 compliance and a seamless transition to 'In life' management. APSU use the PRINCE2 methodology, in common with its use by many leading IT companies, public sector organisations and government agencies.

As a first step we conduct an audit of your existing infrastructure to understand and identify components relevant to PCI DSSv2. We are then able to de-scope the 'in scope network' or 'Cardholder Data Environments' (CDE) and will consult with you to ensure we deliver a lower cost and reduced risk to your business, whilst minimising downtime.

What do we cover?

- Core - network security and server security across all PCI DSSv2 requirements.
- Log management and file integrity monitoring.
- Perimeter security.
- Intrusion prevention systems (IPS) for network, servers and desktop devices.
- Vulnerability assessment tools.
- Penetration testing and approved security vendor (ASV) scans and remediation.
- Network, server and security management platforms.

If your business transacts cardholder data, then your business relies on IT and you can rely on us.

For further **information** contact our sales team on **01285 862 100** or email **info@apsu.com**