

PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is supported by all the global card brands including Visa, MasterCard and American Express. Any company storing, processing or transmitting cardholder data must be compliant with the PCI DSS or risk losing their ability to process credit card payments. As well as applying to merchants, the PCI DSS also applies to service providers and issuing banks.

IRM is a Qualified Security Assessor Company (QSAC) and a Qualified Forensics Investigator (QFI) for all payment cards and has specialist consultants with full QSA status available to advise clients on all aspects of their route to PCI DSS compliance as well as conducting formal PCI DSS assessments.

Complying with the PCI DSS often involves changes to technology, however the greater challenge is the change that will be required to people and processes within the organisation. As such, leadership of the PCI DSS compliance programme requires sponsorship from the executive and ownership from your key business unit, usually Finance and/or Treasury. IRM has considerable experience at working with teams to obtain this buy-in from senior executives, and can work with you to ensure this is obtained.

A PCI DSS remediation programme will usually involve all parts of your business, hence the strong leadership requirement and consistent communication to engage all people (staff and third parties) involved in handling cardholder data for any purposes.

IRM offers the following services to help your PCI DSS compliance programme:

- **PCI DSS Permeation Exercise**

Without knowing where your cardholder data touches your systems it is impossible to clearly define the scope for any remediation activities. During a permeation exercise, IRM will attempt to enumerate all routes cardholder data takes through your networks, creating a permeation map that can be used to form the scope of a PCI DSS programme.

- **PCI DSS Healthcheck**

This is a high-level look at your organisation's posture in relation to PCI DSS compliance. Generally, this will take the form of a series of structured interviews with key stakeholders to determine the current state of the PCI DSS compliance programme, and any areas where remediation will be required. The healthcheck is a useful exercise during the early stages of a PCI DSS compliance programme to highlight areas of weakness and help focus a suitable remediation plan.

- **PCI DSS Pre-Audit**

During a pre-audit, IRM examines the cardholder data environment in detail against the requirements of the PCI DSS to ensure that there are no 'failing elements' within scope and that any remediation projects have been successfully completed.

- **PCI DSS Audit**

During a formal audit, IRM will follow the PCI Security Standards Council's audit procedures to produce a formal report on compliance (RoC) based on your environment. At this stage, all remediation should be complete or the environment will fail the formal audit.

Our PCI DSS service offerings can be tailored to meet the needs of the organisation concerned. IRM is able to offer versatile consultancy both before and during the implementation of any remediation plan. Please contact us to discuss your needs.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.