

The PCI Data Security Standard (DSS)

PCI DSS is a worldwide information security standard aimed at protecting customer card holder data. Compliance with PCI DSS is mandatory for any organisation that stores, processes or transmits card holder data.

The scope of PCI DSS compliance is significant, both in terms of effort and costs. Enterprises are seeking ways to control costs, simplify, and speed up PCI DSS compliance. One proven, effective approach to fast-track compliance is a PCI training programme for all staff involved with PCI compliance.

Mustard Security Training

Mustard has a long-established track record of providing high quality security training to global banks and financial institutions. PCI DSS Training, which is now a core part of this programme, was introduced to assist clients in lightening the load of PCI compliance and to facilitate cost-effective compliance programmes.

How PCI Training Can Fast-Track Compliance

Without formal PCI Training, many organisations go through a steep “learning experience” for all staff involved in compliance. This can result in a slow and disjointed compliance programme with effort sometimes being applied in the wrong places and to the wrong levels, whilst critical parts of the infrastructure are left untouched.

PCI DSS Training ensures that all staff fully understand the detail of compliance - what is important and what is not - and what is “behind” the twelve major requirements of DSS. This allows the proper analysis and prioritisation of the compliance programme in an organisation.

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire

Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 1.2 October 2008

The Prioritized Approach to Pursue PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations. By its comprehensive nature, the standard provides a large amount of information about security – so much that some people who are responsible for cardholder data security may wonder where to start the continuous journey of compliance. Toward this end, the PCI Security Standards Council provides the following Prioritized Approach to help stakeholders understand where they can act to reduce risk earlier in the compliance process. No single milestone in the Prioritized Approach will provide comprehensive security or PCI DSS compliance, but following its guidelines will help stakeholders to expedite the process of securing cardholder data.

HIGHLIGHTS

- Can help merchants identify highest risk targets
- Creates a common language around PCI DSS implementation and assessment efforts
- Milestones enable merchants to demonstrate progress on compliance process

What Is the Prioritized Approach?

The Prioritized Approach provides six security milestones that will help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance. The Prioritized Approach and its milestones (described on page 2) are intended to provide the following benefits:

- Roadmap that an organization can use to address its risks in priority order
- Pragmatic approach that allows for “quick wins”
- Supports financial and operational planning
- Promotes objective and measurable progress indicators
- Helps promote consistency among Qualified Security Assessors

Objectives of the Prioritized Approach

The Prioritized Approach provides a roadmap of compliance activities based on risk associated with storing, processing, and/or transmitting cardholder data. The roadmap helps to prioritize efforts to achieve compliance, establish milestones, lower the risk of cardholder data breaches sooner in the compliance process, and help acquirers objectively measure compliance activities and risk reduction by merchants, service providers, and others. The Prioritized Approach was devised after factoring data from actual breaches, and feedback from Qualified Security Assessors, forensic investigators, and the PCI Security Standards Council Board of Advisors. It is not intended as a substitute, short cut or stop-gap approach to PCI DSS compliance, nor is it a mandatory one-size-fits-all framework applicable to every organization. The Prioritized Approach is suitable for merchants who choose an on-site assessment or use SAQ D.

© 2008 PCI Security Standards Council LLC. The intent of this document is to provide supplemental information, which does not replace or supersede PCI DSS Security Standards or the supporting documents. 2/08

VISA

MasterCard

AMERICAN EXPRESS

Diners Club International

DISCOVER NOVUS

JCB

PCI DSS Integration With Standard ISMS

Many organisations have an existing Information Security Management System (ISMS) or security compliance programme such as ISO 27001. It is important to understand how PCI compliance can fit in with an existing programme and how it can strengthen the programme rather than complicate it.

PCI DSS Training identifies the overlaps with common ISMS such as ISO 27001 and shows how PCI can be fully integrated with a risk-based security assessment and audit programme.

Courses Available

Mustard have developed a modular PCI DSS training course to address the needs of a wide variety of organisations. Your organisation can build a custom training course by selecting from the modules available or have a balanced one-day course which covers the breadth and depth of PCI DSS.

Courses can be run on-site in your location or in a location convenient to you and your organisation.

Who Should Attend?

The course is suitable for both technical and non-technical staff from:

- IT Security, IT Staff and Systems Architects
- Application and Web Developers
- Network Architecture and Operations
- PCI DSS Programme Managers & Stakeholders
- Audit & Compliance
- Finance and HR
- Senior Management
- Business Analysts

Standard One-Day Course Coverage

- History, scope & importance of PCI DSS
- Who's affected – Service Providers, Merchants
- Consequences of non-compliance
- Common myths about PCI
- Quick compliance tips and techniques
- Top reasons for failing compliance
- Study of the “Digital Dozen” requirements
- Self Assessment Questionnaires (SAQs)
- Handling a breach – do's and don'ts
- Approved Scanning Vendors (ASVs) – what they do and how to select them
- Qualified Security Assessors (QSAs) – What they do, how and when to select them
- Remediation tools and techniques
- Tools to speed compliance
- Web application vulnerabilities
- PCI .vs. ISMS such as ISO 27001
- Security Policies

Availability and Booking

The standard one-day PCI DSS Training course is run every two weeks and can be booked by calling Manisha on 0207 357 7300 or emailing: manisha.marsh@mustardresearch.com

Alternatively, please ask for one of our consultants to call you to discuss a bespoke training course to match your requirements.