

The PCI Implementation Workshop will help participants understand the requirements of Payment Card Industry Standards and learn the implementation through interactive case studies. This workshop is primarily oriented to enable participants to implement PCI Standards successfully and enable them to be certification ready.

## Who should attend?

**Relevant Industry Verticals:** Banks, Third Party Processors, IT companies, Telecommunication, Retail, Web hosting Companies and others **dealing with Card Holder Information.**

**Pre-requisite:** Basic Knowledge of Information Security.



14hrs CPE  
Credit

## Why should you attend?

- Data Security has grown in its relevance in today's information security requirements.
- Understand the requirements of PCI DSS and learn the implementation through interactive case studies.
- Intense, detailed curriculum covering all aspects of PCI Implementation challenges.
- Receive useful PCI DSS checklist handouts and courseware
- Learn all about the Payment Card Industry and the processing of transaction, data flow, data compromise.
- Mentoring by highly experienced and the most sought after PCI Assessor.
- **CPISI** certification (**Certified Payment-Card Industry Security Implementer**) on successful completion of the exam at the end of the training program.
- **14 hrs** CPE credit for the CISA / CISM / CISSP

*N.B. Each main topic is presented as a lecture session followed by an exercise to ensure full understanding and consolidate the key learning points. Participants are encouraged to try out the implementation of PCI DSS requirements in the classroom environment.*

## A brief description of the course:

The course is highly participative and follows a tried and tested format which alternates lecture sessions with practical exercises in breakout groups. The subject areas are:

- PCI-DSS background and consequences of non-compliance.
- Scoping and Overview of all the 12 requirements of PCI DSS.
- Case study & detailed discussion on each requirement.
- Relation between PCI DSS and PA DSS.
- Overview of all the 14 requirements of PA DSS with their mapping to PCI-DSS.
- **Examination and Certification (CPISI)**



CPISI

The PCI DSS framework is divided into 12 security requirements (VISA refers to them as the 'Digital Dozen') which are organized in six categories as follows:

**1) 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

**2) Protect cardholder data**

**Requirement 3:** Protect stored cardholder data

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

**3) Maintain a vulnerability management program**

**Requirement 5:** Use and regularly update anti-virus software or programs

**Requirement 6:** Develop and maintain secure systems and applications

**4) 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

**5) 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

**6) Maintain an information security policy**

**Requirement 12:** Maintain a policy that addresses information security for employees and contractors

- Test
- Closing Discussion (Experiences and Information sharing)

**Highly Experienced Workshop Leader:**



**Mr. Dharshan Shanthamurthy**

CISSP, CISA, ISO 27001LA, NSP (CERT®), PCI Qualified Security Assessor, CEH, OCTAVE® (SEI-CMU) Trainer and Advisor, BCM Trainer, VISA QPASP, Payment Application Qualified Security Assessor.

Dharshan is a subject matter expert on Payment Card Industry Standards including the PCI DSS and PA-DSS. Having conducted more than 50 workshops globally on PCI DSS, OCTAVE, PA-DSS, BCM and ISO 27001, he is one of the well known trainers in information security in Asia Pacific region. Dharshan has lead PCI assessment for over 22 organizations ranging from large IT Companies, BPO's, Banks and Processors. He brings in hands on knowledge of PCI DSS Implementation for organizations.

**Overview**

The **Payment Card Industry Data Security Standard (PCI-DSS)** is a compliance initiative from the Payment Card Industry Standard council (PCI-SSC). PCI SSC is a body formed by major payment brands in the world namely MasterCard, VISA, American Express and Discover that dictates best-practice security standards. The standard involves on-site audits, self-administered audits, and network scanning, not all of which apply to everyone.

**As per PCI-DSS all Banks, Merchants, Service Providers, Web Hosting Companies, Transaction Processors who are processing, storing, transmitting or switching cardholder data have to comply with PCI DSS standard.** If the organization fails to comply with this standard and if a fraud were to be perpetrated in any of these organizations, Payment Brands will hold these organizations (namely Banks, Merchants, Hosting Companies) liable for penalty and legal action apart from severe reputation loss.