Payment Card Industry Data Security Standard (PCI DSS)

Course Outline

SPARTAN
Allied Services
Deliver Results - Create Value

www.saservices.com.ph

Program Overview

PCI DSS Training is an essential part of any PCI DSS Compliance program, whether you are a merchant, service provider, bank or issuer. Our PCI DSS Training courses will arm you with the necessary PCI DSS know-how so you can confidently scope, assess and advise on your own unique environments.

The courseware has been developed upon the Visa PCI DSS manual which served as the basis for the Qualified Security Assessor (QSA) Training Course developed by the PCI SSC and fully covers all topics included on the QSA and ISA certification exams. From a practical standpoint, our Advanced PCI DSS Training Course far exceeds the basic training provided by the PCI SSC and Card Issuers, which can leave you with more questions than you started out with in the first place

Duration

2- Day Program

Learning Objectives

At the end of this training, participants should be able to:

- A unique opportunity to take a QSA Auditor's perspective on scoping, gap analysis, remediation and assessment issues.
- Gain an in-depth understanding of the PCI DSS standard and its relation to other PCI standards such as PTS DSS and PA DSS.
- Save time and reduce costs in preparation for a formal On-site Validation Assessment or completion of a Self-Assessment Questionnaire.
- Through better understanding and deeper knowledge make informed decisions about managing compliance in-house vs outsourcing, utilizing open source vs. commercial solutions.
- Learn how to avoid typical pitfalls on the path to achieving compliance and how to adopt a program versus project based approach to maintaining an ongoing compliant posture.
- Interactive Q&A sessions, workshops and case studies will enable participants to demystify questions specific to their organization and environments.
- Empower your organization with key skills that can reduce reliance on third party advice, consequently reducing consultancy costs.
- Network and interact with attendees facing similar challenges within their organizations. Exchange ideas, share experience about products, vendors and consultancy organizations.

Target Audience

Audit Managers, Business Analysts, Compliance Officers, Credit Analysts, Finance Managers, IS Managers, IT Specialist, Project/ Program Managers, Risk Management Analysts, Security Analysts, Senior Developers, Software Engineers, System Administrators and Web Masters

Program Structure and Outline

The Program is delivered using a combination of instructor-led lectures, case study and exercises on practical implementation of the concepts discussed within the training. The topics presented below define the areas of focus under the program.

DAY 1

Module 1:

- Overview of the PCI DSS
- Understanding Security
- DSS Lifecycle Process
- Requirements versus Frameworks

Module 2:

Security Breaches Overview & Vulnerability Experiences Current statistics and examples Impact of Data Compromises and Increasing Risk to Cardholder Data Compromise Case Study Examples

Module 3:

PCI DSS and related standards DSS Objectives Relationship to Industry Standards Compliance & Validation – key differences Payment Application Scope

Module 4:

PCI DSS Applicability and Scoping Important Cardholder Data concepts PCI DSS Scoping Statement Network Segmentation, Scoping examples

Module 5:

Compliance Validation Process What is PSR/AIS Compliance and Validation Levels Compliance versus Validation Overview of Scoping, Sampling and Compensating Controls

Module 6:

- PSR/AIS Compliance Programs
- Security Initiatives & Industry Collaboration
- Merchant Levels and Validation Requirements

Module 7:

- Industry Players & Transaction Lifecycle Important Definitions – Entities involved
- Important Definitions – Transaction Flow
- Transaction Flow – Authorization, Clearing, Settlement

Module 8:

Cardholder Data, Finding and Eliminating Sensitive Authentication Data CVV vs CVV2, Track 1 vs Track 2 Data, Full Track or Magnetic Stripe Track Data Characteristics and Guidelines for Searching, MOD-10 (The Luhn Formula) The PCI PIN Transaction Security Program

Module 9:

Compensating Controls Definition, Myths, Facts Successfully Applying Compensating Controls, Analyzing Risk Case Study Scenario and Discussion

Module 10:

- PCI SSC Quality Assurance Program
- Program Intent & Lifecycle
- QA Scoring Matrix
- Program Feedback and Violations Investigation

Module 11:

- Approved Scanning Vendors (ASVs)
- What is an ASV, Pass and Fail ASV Certification Criteria
- Common Vulnerability Scoring System (CVSS)
- Scan Report Analysis

Module 12:

- New Standards and Emerging Technologies
  - 12.1 Data Field Encryption / E2EE / P2PE
  - 12.2 Wireless Network Guidelines
  - 12.3 Virtualization & Cloud Computing
  - 12.4 Tokenization

Module 13:

- Call Centre Environments
  - 13.1 Desktop Environment Scope
  - 13.2 Call Recordings – SAD Data

Module 14:

- Risk Assessment
- What is a Risk Assessment with regards to PCI DSS
- Risk Assessment Drivers
- Risk Assessment Methodologies

DAY 2

Detailed explanation of PCI DSS Requirements and Audit Guidelines for all 6 Domains, containing the 12 Sections and related sub requirements including:

- PCI DSS Section 1 – Install and maintain a firewall configuration to protect cardholder data
- PCI DSS Section 2 – Do not use vendor-supplied defaults for system passwords and other security parameters
- PCI DSS Section 3 – Protect stored cardholder data
- PCI DSS Section 4 – Encrypt transmission of cardholder data across open, public networks
- PCI DSS Section 5 – Use and regularly update anti-virus software
- PCI DSS Section 6 – Develop and maintain secure systems and applications
- PCI DSS Section 7 – Restrict access to cardholder data by business need-to-know
  PCI DSS Section 8 – Assign a unique ID to each person with computer access
- PCI DSS Section 9 – Restrict physical access to cardholder data
- PCI DSS Section 10 – Track and monitor all access to network resources and CHD
  PCI DSS Section 11 – Regularly test security systems and processes
- PCI DSS Section 12 – Maintain a policy that addresses information security
- Q&A

Why Choose SAS Management Inc.

We Deliver Results

SAS Management Inc. has consistently proven its capability to deliver and exceed our clients' expectations. We are the only PEOPLECERT© Accredited Training Organization (ATO) in the Philippines. Our pool of consultants and trainers are seasoned industry veterans who have above average qualifications and certifications such as Business Management, Process Improvement, and Organizational Development Programs.

We Create Value

SAS Management Inc. believes in ensuring that our services meet the intended needs of our clients. To us, it is more than just providing training and consulting but rather ensuring that these are the things that our clients really need. This is why SAS Management Inc. is probably the only training provider that does a thorough needs assessment prior to providing a proposal. Our goal for every proposal is to CREATE VALUE for your organization.

SAS Management, Inc. is affiliated and endorsed by the following organizations:

Key Affiliations/Accreditation

Key Partner Programs

Key Partners