CERTIFIED PAYMENT SECURITY PRACTITIONER (CPSP) TRAINING

PCI DSS v3.2.1 CERTIFICATION TRAINING COURSE

FOR ASIA & MIDDLE EAST
DATES: 9th, 10th & 11th JUNE, 2020
TIME: 2.00 PM to 6.00 PM (GMT +8)

MODE: ONLINE
COURSE FEE:
ISACA Members: USD $ 100
Non-ISACA members: USD $ 120
EARN 12 CPE CREDIT POINTS

FOR AMERICAS & EUROPE
DATES: 15th, 16th & 17th JUNE, 2020
TIME: 2.00 PM to 6.00 PM (GMT +1)
INTRODUCTION

Payment Card Industry Data Security Standard (henceforth termed as PCI DSS) is developed to promote and facilitate payment card holder data security. The standard applies to business entities such as but not limited to merchants, payment processors, issuers, acquirers, service providers which store, process and/or transmit payment card data.

WHO SHOULD ATTEND?

- Chief Information Security Officers
- Compliance officers
- Information Technology Managers
- Developers Information Systems & Security Implementer
- Other Security Professionals

IMPORTANCE OF PCI DSS

The standard works as an enabler for organizations to implement security controls to provide reasonable data security assurance while processing payment card transactions. The PCI DSS compliance guides organizations by providing a set of baseline technical and operational security controls which can be integrated as a “business as usual (BAU)” process in the organization. The way payment ecosystem and its associated technology are changing it is becoming massively important for organizations to have a “Sustainable Payment Card Security Compliance Program” and PCI DSS compliance helps you by providing a much-needed framework to build a credible payment card data security program.

WHY CPSP?

In the past few years, we have seen massive breaches at organizations such as Target and Equifax. In many cases, these organizations were compliant to PCI DSS. Yet, breaches happened and in most cases, the breach was notified to the impacted company by an outside agency. Investments in complying to these standards are in addition to technology investments made by companies in anti-viruses, firewalls, security incident and event management systems, etc. The traditional checkbox approach to cybersecurity no longer works.

It is important that organizations realize that the cybersecurity journey goes far beyond just compliance to any given standard. Organizations should also recognize that even after significant investments breaches can still occur.

The training will cover the entire payment ecosystem and the latest PCI DSS standard which will help participants in understanding the intent and objective of each PCI DSS requirement. The training will also provide participants with a platform where they can understand a PCI QSA’s (Payment Card Industry Qualified Security Assessor) perspective of validating a PCI DSS requirement.

The training will provide participants a hands-on experience of implementing PCI DSS compliance program through case studies and examples.

OBJECTIVE OF PCI DSS COMPLIANCE PROGRAM

- Building a framework for securing payment card data
- Ensuring security and not just compliance
- Taking a risk-based approach to implement security controls
- Winning end customer trust
- Going beyond the traditional checklist-based approach for security

In line with these objectives, we are pleased to announce a 3-day training on “Certified Payment Security Practitioner (CPSP)”. 
Certified Payment Security Practitioner (CPSP) Course

COURSE CONTENT

PART 1:
- Basics of Payment Ecosystem: Card Data (Track data, EMV Chip), Entities involved
- Payment Transaction flow: Issuing and Acquiring (Card Present and Card Not Present Transactions)
- Stages of Payment Processing: Authentication, Authorization, Clearing, Settlement, Chargeback, Refund etc.
- Various Payment Channels: ATM, POS, Ecom, Mobile App, MOTO, NFC or Contactless
- PCI Perspective on architecture: Good and Bad: Inhouse Arch., Third party Cloud Architecture, Virtualization
- What is PCI DSS
- Who is PCI SSC
- Responsibilities of various entities: PCI SSC, PCI QSAs, PCI ASVs etc.
- PCI DSS Compliance Mandate and Applicability of PCI DSS
- Levels of Service Provider and Merchants
- Various SAQs and Applicability
- PCI DSS and Card Data Storage Mandate: A Glimpse

PART 2:
- Overview PCI DSS v3.2.1: 6 objectives and 12 Requirements
- Overview of PA-DSS
- Overview of PCI PTS
- Overview of PCI P2PE
- Integration Model for Various PCI Standards
- PCI DSS Scoping and Network Segmentation
- Scoping vs Sampling: What is what?
- PCI DSS Risk Assessment Methodology and Approach
- PCI DSS and ISO 27001: A Comparison

PART 3:
- Implementing PCI DSS Requirements: Detailed discussion on each requirement and sub requirement of PCI DSS v3.2.1
- QSA Perspective for each PCI DSS requirement and Best Practices
- PCI DSS Using Open Source tools: Suggestion on available tools to meet PCI DSS requirements
- Appendix A1 and A2
- Designated entities supplemental validation (DESV)
- Overview and implementation practices of Compensating Controls
- Implementing PCI DSS control while working from home.
- What kind of threats are prowling online related to the COVID-19 crisis?

PART 4:
- Annual PCI DSS Compliance
- Management: The PCI DSS Calendar
- An Approach to Handle suspected card data breach
- PCI DSS Resources and Knowledge Library
- What to look for in a PCI QSAC?

Examination – The participants would need to undergo an online examination after the training. On successful passing of the examination (minimum 60%) the participant would be awarded the certification.
OUR TRAINERS

Nikhil Raj Singh brings in 10+ years of experience working in the payment security space. Currently, he is a PCI QSA working with Network Intelligence as a lead consultant and trainer. He has got vast experience in implementation, remediation and certification of PCI DSS for companies across the globe operating in the verticals of Banking, Financial Services, Airlines, BPOs, Telecom and so on. His hands-on experience working in the payment security domain helps his audience connect to the real-life scenarios and understand the practical applications of the PCI Controls.

Deep Chanda brings in about 15+ years of experience working in the payment security space. Currently Deep is working as Business head & is leading the Payment security vertical at Network Intelligence. Being from an Information security background, Deep is well versed of the challenges faced by the organizations and has helped companies to reduce their efforts and costs for attaining PCI compliance.

REGISTRATION FORM FOR ASIA & MIDDLE EAST

Click Here For Registration

REGISTRATION FORM FOR AMERICAS & EUROPE

Click Here For Registration

PRIVACY NOTICE & CONSENT:

We are committed to respecting your privacy and we recognize the importance of protecting the information collected about you. All of the personal information that you have submitted during the registration shall only be processed in relation to your attendance to this event (i.e., processing of payments, issuance of certificate, sending of any announcements, future events and activities). Trainings will be recorded and shall be use for internal purpose.

All the information that you have provided in relation to this event shall be protected with reasonable and appropriate measures, and shall only be retained as long as necessary in its processing. I have read, accept and agree to the privacy policy.

I agree to pay the total amount due above for my registration and I have read, accept and agree to abide by all the terms and conditions stated on this document.