NETWORK INTELLIGENCE
Global cybersecurity provider

CERTIFIED PAYMENT SECURITY PRACTITIONER (CPSP) TRAINING

A 16 hour PCI DSS Certification Workshop

INTRODUCTION

Electronic payments have witnessed a revolution over the last two decades and to improve the safety of the card holder data and to combat credit card frauds and breaches, the 5 major card brands came together in 2004 and formed the Payment Card Industry Security Standards Council (PCI SSC) to introduce a common payment security standard – PCI DSS.

Payment Card Industry Data Security Standard (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

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 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. By following the framework and implementing the necessary controls, you can keep your data secure, avoid costly data breaches and protect your employees and your customers.

NETWORK INTELLIGENCE
Global cybersecurity provider

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 CPSP 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 CPSP 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 CPSP 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
- Guidance to professionals for protecting customer data
- Ensuring security and not just compliance
- Going beyond the traditional checklist-based approach for security
- Taking a risk-based approach to implement security controls
- Winning end customer's trust

In line with these objectives, we are pleased to announce a 4-day 4-hour online training on "Certified Payment Security Practitioner (CPSP) ".

Certified Payment Security Practitioner (CPSP) Training

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
- Approach for PCI DSS Implementation and Certification: "The Phased Approach"
- 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

NETWORK INTELLIGENCE
Global cybersecurity provider

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 QSA ?

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.

" Prevent a security breach by keeping data out of reach "

NETWORK INTELLIGENCE
Global cybersecurity provider

Lead Trainer

Nikhil Raj Singh,
Payment Security - Delivery Lead,
Network Intelligence

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.

REGISTRATION FORM : https://forms.office.com/r/jkWWsiftsF