NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Payment Security Practitioner (CPSP v2.0) Training

Learn the changes and advances in latest version of PCI DSS v4.0

Batch 1: Americas & Europe

Dates: May 16-19, 2022

Time: 1:00 PM To 5:00 PM (GMT)

Mode: Online

Batch 2: Asia & Middle East

Dates: May 23-26, 2022

Time: 6:00 AM To 10:00 AM (GMT)

Mode: Online

Course Fees:

Regular Participant : USD $ 175

ISACA/ISC2 Members : USD $ 150

NETWORK INTELLIGENCE
Global cybersecurity provider

C P S P
Certified Payment Security Practitioner

Introduction

The PCI Data Security Standard (PCI DSS) is a global standard that provides a baseline of operational & technical requirements designated to protect payment data. PCI DSS v4.0 is the next evolution of the standard.
PCI DSS v4.0 replaces version 3.2.1 to address emerging threats and technologies and enable innovative methods to combat new threats. This version associate the protection of payment data with new controls to address sophisticated cyber attacks.

What is new in PCI DSS v4.0

- Meeting the security needs in PCI continuously
- Promoting security as a continuous process
- Adding flexibility and support of additional methodologies to achieve security
- Enhancing validation methods and procedures

Why PCI DSS v4.0 is important?

- As threats change, New version of security practices must evolve.
- Ongoing security is crucial to protect the payment data always as criminals never sleep.
- Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.
- To support transparency and granularity, must have a clear validation and reporting options.

NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Payment Security Practitioner

Why CPSP v2.0?

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 v2.0 training will cover the entire payment ecosystem and the latest PCI DSS v4.0 standard which will help participants in understanding the intent and objective of each PCI DSS v4.0 requirement. The CPSP v2.0 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 v4.0 requirement.

Objectives 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

NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Payment Security Practitioner

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 v4.0 ?
- Who is PCI SSC v4.0?
- Responsibilities of various entities: PCI SSC, PCI QSAs, PCI ASVs etc.
- PCI DSS v4.0 Compliance Mandate and Applicability of PCI DSS v4.0
- Levels of Service Provider and Merchants
- Various SAQs and Applicability
- Approach for PCI DSS v4.0 Implementation and Certification: “The Phased Approach”
- PCI DSS v4.0 and Card Data Storage Mandate: A Glimpse

PART 2:

- Overview PCI DSS v4.0: 6 objectives and 12 Requirements
- Overview of PA – DSS, PCI SSF
- Overview of PCI PTS
- Overview of PCI P2PE
- Integration Model for Various PCI Standards
- PCI DSS v4.0 Scoping and Network Segmentation
- Scoping vs Sampling: What is what?
- PCI DSS Risk Assessment Methodology and Approach
- PCI DSS v4.0 and ISO 27001: A Comparison
- PCI DSS v 3.2.1 VS v4.0
- PCI DSS v4.0 timelines

NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Payment Security Practitioner

PART 3:

- Implementing PCI DSS v4.0 Requirements: Detailed discussion on each requirement and sub requirement of PCI DSS v4.0
- QSA Perspective for each PCI DSS requirement and Best Practices
- PCI DSS v4.0 Using Open-Source tools: Suggestion on available tools to meet PCI DSS v4.0 requirements
- Appendix A1 and A2
- Designated entities supplemental validation (DESV)
- Overview and implementation practices of Compensating Controls
- Customized Approach

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

PART 4:

- Annual PCI DSS v4.0 Compliance
- Management: The PCI DSS v4.0 Calendar
- An Approach to Handle suspected card data breach
- PCI DSS v4.0 Resources and Knowledge Library
- What to look for in a PCI QSA ?

In line with these objectives, we are pleased to announce a 4-day 4-hour online training on “Certified Payment Security Practitioner (CPSP v2.0) ”.

NETWORK INTELLIGENCE
Global cybersecurity provider

Certified Payment Security Practitioner

Trainer Details

Udit Pathak,
Principal Consultant – Compliance and Audit,
Network Intelligence

Udit Pathak currently serve as Principal Consultant at Network Intelligence focusing on Information Security audits (PCI DSS, ISO 27001, HIPAA, cloud security, PCI SSF, PA DSS, PCI PIN etc.), Data privacy audit and implementation, application security assessment, vulnerability assessment (IT infrastructure and various components), technical security audits, security configuration review, security /privacy maturity assessment etc.. He has delivered excellent projects across the globe on Payment eco system, BFSI, travel industry, health care, defence services etc.

Mufaddal Taskin
Cybersecurity Training Specialist
Network Intelligence

Mufaddal has over 26 years of diverse experience in technology solutions and cyber security. He currently serves as a cybersecurity Training Specialist at NI His work mainly focuses on Payment Security Audits Security Trainings, Vulnerability Assessment and Penetration Testing for NI. His technical abilities span across Networks, Web Apps, Incident Response, Cyber Threat Intelligence, SOC and ISO standards Compliance. Mufaddal has created custom course outlines as well as conducted the same for a variety of high technologies clients of NI.

Registration Link : https://forms.office.com/r/VFuy0r51Mv