Certified Payment Security Practitioner (CPSP v2.0)

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

Batch 1: Asia & Middle East
Date : 22- 25 January 2024
Timing: 6:00 am – 10:00 am GMT
Mode of training: Online

Batch 2: Americas & Europe
Date: 29 January – 1 February 2024
Timing: 2:00 pm – 6:00 pm GMT
Mode of training: Online

Course Fee:

USD 200 for regular participants

USD 150 for ISACA/ISC2 members

NETWORK INTELLIGENCE
The Digital Security Company

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 associates 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 versions 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 clear validation and reporting options.

Please note that the PCI DSS 3.2.1 expires in March, it's essential to stay updated on the latest developments and announcements from the PCI Security Standards Council (PCI SSC).

©2022 Network Intelligence. All rights reserved.

Why CPSP v2.0?

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.

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

Objectives of the 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 implementing security controls
- Winning end customer's trust

©2022 Network Intelligence. All rights reserved.

Course Content

Day 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?
- 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 Providers 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

Day 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

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

©2022 Network Intelligence. All rights reserved.

Day 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

Day 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 announce a 4-day 4-hour online training on "Certified Payment Security Practitioner (CPSP v2.0) ".

©2022 Network Intelligence. All rights reserved.

Trainer Details

Udit Pathak,
Head of Department– Compliance and Audit,
Network Intelligence

Udit has rich experience of 10+ years in the field of information security and Audits. He has carried out PCI DSS audits, ISO27001, Vulnerability assessments, System and Server Audits, Web application security assessments, Secure code reviews, Technical security assessments, Vendor Audits, HIPAA Implementation & Audits, and SOC maturity assessments. Udit heads the Compliance & Audit Delivery channel at Network Intelligence. He has delivered excellent projects across the globe for the payment ecosystem, BFSI, the travel industry, health care, and defense services for both cloud and traditional on-prem solutions.

Registration Link: https://forms.office.com/r/ycsay8csja