



Certified Payment
Security Compliance
Manager



Certified Payment Security Compliance Manager (CPSCM)

Join our CPSCM Workshop for comprehensive learning of the entire PCI Suite including PCI DSS, PCI PIN, PCI 3DS, PCI SAQ, UPI, Mobile Wallets, SWIFT and beyond.

REGISTER NOW

 **WEBSITE**

COURSE FEE:

\$130

REGULAR
PARTICIPANTS

\$100


ISACA/ISC2
MEMBERS

\$80

RETURNING
PARTICIPANTS/
CLIENTS

SLOTS


ASIA & MIDDLE EAST

 **06th May to 9th May, 2024**

 **6:00 AM - 10:00 AM GMT**

AMERICAS & EUROPE

 **13th May to 16th May, 2024**

 **3:00 PM - 7:00 PM GMT**

16 Hours of Live Interactive
Workshop (4 Days 4 Hours)

IN PARTNERSHIP WITH



ISACA® I(ISC)™



Introduction of CPSCM

In an ever-evolving digital landscape, the security of payment transactions is of paramount importance. The Certified Payment Security Compliance Manager (CPSCM) workshop program is meticulously designed to empower professionals with the knowledge and skills necessary to navigate the complexities of the payment industry and ensure robust security measures.



What to Expect?



DAY 1: Building the Foundation

Dive into the background and evolution of the payment industry, understanding the intricacies of payment transaction flows, and exploring the roles and responsibilities of entities within the payment ecosystem. Get acquainted with the various form factors for payment and payment channels, staying up-to-date with the latest changes in PCI DSS v4.0.



DAY 2: Understanding the PCI Suite of Standard

Delve into the details of PCI DSS requirements, from data discovery to compensating controls. Explore a unified compliance approach, and gain insights into the broader suite of payment standards beyond PCI DSS, including PCI PIN, PCI 3DS, PCI P2PE, PCI CP, SSF, and SWIFT.



DAY 3: Emerging Payment Technologies

Uncover the intricacies of SWIFT, UPI, Mobile Payments, QR Codes, and Contactless Payments. Learn their architectures, security measures, transaction flows, and global adaptability, ensuring a comprehensive understanding of the diverse landscape of modern payment technologies.



DAY 4: Maintaining Compliance

Grasp the nuances of maintaining compliance, the frequency of activities for PCI DSS annual revalidation, and the crucial aspects of report review. Explore the PCI DSS resources and knowledge library, culminating in a practical case study to reinforce your understanding.



Key Topics Covered

- » **Background and Evolution of the Payment Industry**
- » **Various form factors for payment and Payment Channels**
- » **What's new with PCI DSS v4.0**
- » **PCI DSS – On-Prem, Cloud, Shared – What's Different?**
- » **Risk Assessment**
- » **Self-Assessment Questionnaire (SAQ)**
- » **Implementing PCI DSS requirements**
 - Detailed discussion on Requirement 1 To 12 of PCI DSS and sub-requirements
- » **Overview of all the other Payment and PCI suite of standards**
 - PCI PIN, PCI 3DS, PCI P2PE, PCI CP, SSF and SWIFT
- » **UPI – Unified Payment Interface**
- » **Mobile Payments**
- » **QR Codes**
- » **Contactless Payments**
- » **Maintaining compliance**
- » **CPSCM – Multiple Choice certification exam**



Table of Contents

DAY 1

▶ **Background and Evolution of the Payment Industry**

- Elements of the card and importance of card data (Track data, CCV, PAN, PIN)
- Payment transaction flow (Card present and Card not present)
- Stages of payment processing (Authentication, Authorization, Clearing and Settlement)
- Roles and responsibilities of various entities involved in the payment ecosystem
- PCI SSC and responsibilities/differences b/w ISA, QSA, PCI SSC and ASV

▶ **What's new with PCI DSS v4.0**

- Transition timelines – v3.2.1 to v4.
- Goals and summary of changes

▶ **PCI DSS – On-Prem, Cloud, Shared – What's Different?**

- Type of PCI DSS environments
- What to look for when hosting system components in the different types of cloud environment
- Shared Responsibility Matrix

▶ **Risk Assessment**

- Combination of NIST, OCTAVE, and ISO Risk assessment
- TRA – Targeted Risk Analysis as part of PCI DSS v4.0

▶ **Self-Assessment Questionnaire (SAQ)**

- Merchant and service provider levels
- Applicability and different types of SAQ

▶ **Implementing PCI DSS requirements**

- Detailed discussion on Requirement 1 To 3 of PCI DSS and sub-requirements
- Best practices from a QSA standpoint
- Importance of Data Discovery and other tools to implement PCI DSS requirements



Table of Contents

DAY 2

➤ **Implementing PCI DSS requirements**

- Detailed discussion on requirement 4- 12 of PCI DSS and sub-requirements
- Best practices from a QSA standpoint
- Compensating controls
- Differences b/w Defined and Customized approach
- Unified compliance approach for PCI DSS

➤ **Overview of all the other Payment and PCI suite of standards**

- PCI PIN, PCI 3DS, PCI P2PE, PCI CP, SSF and SWIFT
- Are these standards interrelated?

➤ **PCI 3DS**

- PCI 3DS data flow – Architecture review
- ACS, DS and 3DSS
- Overview of the PCI 3DS requirements and dependency on PCI DSS

➤ **PCI SSF**

- Transition timelines b/w PA DSS and SSF
- Changes b/w PA DSS and SSF
- SSF – S3 and SSLC Applicability

➤ **PCI CP – Logical and Physical**

- Architecture review – Layout (Physical and Logical)
- Overview of requirements



Table of Contents

DAY 3

▶ **SWIFT**

- Different architectures and applicability of SWIFT
- SWIFT - CSCF 2023 framework

▶ **UPI – Unified Payment Interface**

- What is UPI, and what are the advantages of using UPI
- Security behind UPI vs. other form factors of payment
- Sample UPI transaction flow
- Adaptability of UPI as a form factor of payment across the world

▶ **Mobile Payments**

- What are mobile payments
- Advantages of mobile payments
- Security of mobile payments
- Sample mobile payment transaction flow
- Global Adaptability of mobile payments

▶ **QR Codes**

- What are QR Code payments
- Advantages of QR code
- Security of QR code payments
- Sample QR payment transaction flow
- Global Adaptability of QR code payments

▶ **Contactless Payments**

- What are Contactless payments
- Advantages of Contactless payments
- Security of Contactless payments
- Sample Contactless payment transaction flow
- Global Adaptability of Contactless payment



Table of Contents

DAY 4

- ▶ **Maintaining compliance**
 - Requirements overview and summary
 - PCI DSS Annual Revalidation – Frequency of activities to be performed
 - Report review – ROC and AOC. What to look for?
 - PCI DSS resources and knowledge Library
 - Case study – PCI DSS



Trainers Profile



Prajwal Gowda

VP Delivery and workshops

CISA, CISM, PCI QSA, PCI P2PE QSA, PCI 3DS QSA, SWIFT CSP, PCI TSP, ISO 27001 LA, ISO 27001 LI, CPISI – S Master Trainer

Prajwal Gowda, a seasoned cybersecurity professional with 10+ years' expertise, specializes in AI Security and safeguarding organizations from evolving threats. As Chief Technology Officer (CTO) at Ampcus Cyber, he draws on a rich background as a Business Unit Head, excelling in Compliance and Testing services. His proficiency spans PCI, ISO 27001, Software Security Framework, ISMS, Risk Analysis, and more, reflecting a comprehensive grasp of the cybersecurity landscape. Prajwal is a Master Trainer, having conducted 100+ cybersecurity and AI Security sessions globally, workshop over 1000 professionals.



Nikhil Raj Singh

Chief Strategy Officer

PCI QSA, PCI PIN QPA, PCI 3DS Assessor, PCI Secure Software Assessor, PCI Secure SLC Assessor, CISA, CISM, CRISC, CDPSE

Nikhil Raj Singh has over 10+ years of experience in information security and Audits. He has carried out compliance audits, vendor audits, System and Server Audits, Web application security assessments, technical security assessments, ISO27001, and PCI DSS assessments. He serves as Chief Strategy Officer at Ampcus Tech, focusing on Strategy, research, and operations. He has carried out consulting and audit engagements of different compliance standards such as PCI DSS, PA DSS, PCI 3DS, and ISO 27001 for industry verticals such as Banks, Payment Processors, Merchant Aggregators, TSPs, Airlines, e-commerce merchants, BPOs, ODCs, Telecom in US, Europe, Asia Pacific, and the Middle East. Nikhil is a well-respected trainer and speaker who is well-versed in the necessity of AI security and the scrutiny that surrounds this growing technology.

REGISTER NOW

