ics
Innotec Creative Solutions

30 SEPTEMBER - 2 OCTOBER 2025

PCI DSS MASTERCLASS

PAYMENT CARD DATA SECURITY STANDARD 4.0

MOVENPICK HOTEL | WINDHOEK

PCI DSS 4.0 Masterclass 2025

In an increasingly digital banking environment, and with the increasing frequency of cyber threats, organisations handling sensitive payment information must stay compliant with the Payment Card Industry Data Security Standard (PCI DSS) and implement robust cyber-security practices. PCI DSS provides a robust framework for protecting payment data, reducing fraud, and maintaining customer trust. As banks in Namibia adopt newer technologies and expand their digital payment offerings, a comprehensive understanding of PCI DSS 4.0 is essential. This masterclass aims to equip banking professionals in Namibia with in-depth knowledge of PCI DSS 4.0 requirements, best practices for compliance, and strategies for effective implementation within their organizations.

Course Date	30 September - 2 October 2025
Course Duration	3 days
Daily Starting Times	Registration opens at 08h00 and course starts at 09h00
Course Venue	Movenick Hotel, Windhoek
Delivery Mode	In-person expert-led presentations
Accommodation	Not included
Cuisine	Teas and lunches
Investment	Register and pay early to secure a seat: US$1,200 per person *Includes tuition, course materials, curated experiences and sumptuous meals.*
Programme Director	Stanley Austin **T** +44 7815 033375 **E** scaustin@afri-conomie.com
Programme Coordinator	Tidings Chaitezvi **T** +263 772 368 225 / +263 242 339 641 **E** tidings.c@icsafricagroup.com
Registration Contact	Vuyiso Nyoni **T** +263 776 933 564 / +263 242 339 641 **E** vuyiso@icsafricagroup.com
Registration Link	www.icsafricagroup.com

ICS Africa & Africonomie Partnership

ICS Africa and Africonomie have partnered to deliver a comprehensive Payment Card PCI DSS training program in Namibia. ICS Africa brings extensive expertise in information security and compliance training, while Africonomie specializes in providing targeted financial and technological solutions tailored to the African market. By leveraging their combined expertise and local insights, ICS Africa and Africonomie aim to build capacity within Namibia's payment ecosystem, enabling organizations to achieve and maintain PCI DSS compliance effectively and sustainably. This initiative represents a significant step towards bolstering the country's cybersecurity resilience and financial integrity.

Course Participants

Senior Manager and Compliance Officers
IT and Security Professionals
Payment Systems Managers
Risk Management Teams
Any staff involved in payment card processing and security

Course Content

***Day 1*:**

PCI DSS Essentials
- Overview of the Payment Card Industry
- Introduction to the PCI Security Standards
- PCISSC Resources and Website

Overview of PCI DSS
- History and Evolution of PCI DSS
- Purpose and Importance of PCI DSS Compliance
- Key Stakeholders (PCI SSC, Card Networks, QSAs)

PCI DSS versus Cybersecurity Practices
- How PCI DSS Fits Within a Broader Cybersecurity Framework
- Challenges in Aligning Compliance with Security

***Day 2*:**

PCI DSS Compliance Requirements Overview
- 12 Core PCI DSS Requirements
- Overview of Security Domains (Network Security, Access Control, Encryption, Monitoring)

Detailed Review of Key Requirements
- Install and Maintain a Secure Network
- Protect Cardholder Data with Encryption
- Maintain a Vulnerability Management Programme
- Implement Strong Access Control Measures

- Monitor and Test Networks Regularly
- Maintain a Security Policy
- Defining PCI Scope (Systems and Data Involved)
- Scoping Tools and Strategies
-

***Day 3*:**

Preparing for PCI DSS Audits

- Self-Assessment Questionnaires (SAQ) and Attestation of Compliance (AoC)
- Managing Documentation and Evidence
- Conducting PCI DSS Assessments

Maintaining PCI DSS Compliance

- Continuous Monitoring and Security Audits
- Managing Compliance in Hybrid/Multi-cloud Environments

Expected Outcomes

- Enhanced awareness of PCI DSS 4.0 standards
- Practical knowledge for implementing and maintaining compliance
- Strengthened security posture for payment card data
- Improved risk management strategies
- Facilitated dialogue and collaboration among banking stakeholders