AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

PCI DSS v4.0.1 Onsite Assessment for a Cloud-Native Fintech Platform

Assessment Type:
PCI DSS v4.0.1

Assessment Mode:
Hybrid

Entity Type:
Financial Institution

Assessment Duration:
5 Months

Overview

The organization is a technology company based in India that specializes in providing a comprehensive suite of financial technology (fintech) solutions. The organization empowers banks, non-banking financial companies (NBFCs), and businesses by embedding fintech capabilities into their core operations through custom Application Programming Interfaces (APIs).

Core Offerings

- **Banking Solutions:** The organization offers a holistic core banking system that enables financial institutions to roll out customer-centric banking services. This includes customer onboarding, compliance checks, and regulatory requirements.
- **Lending Services:** The organization provides a core lending suite that allows businesses to extend credit lines through various options like Buy Now Pay Later (BNPL) schemes.
- **Payment Solutions:** The organization facilitates smooth payment experiences by offering solutions for payment gateways, card issuance (both physical and virtual), and digital commerce integration.
- **Customization and Scalability:** The organization's APIs are designed to be flexible and customizable, allowing clients to tailor products according to their specific market needs. The platform supports rapid deployment, enabling clients to bring fintech products to market five times faster than traditional methods.

Ampcus Cyber's Approach

Project Initiation and Scoping

Upon formal engagement, Ampcus Cyber's QSA team conducted detailed scoping discussions with key stakeholders to comprehensively understand the organization's requirements and environment complexity. This initial phase was critical given the diverse nature of the environments requiring assessment and the technical sophistication of the infrastructure. The team worked to clearly delineate the cardholder data environment (CDE) boundaries and identify all in-scope systems across multiple cloud platforms.

Due to the complexity of the environments, Ampcus Cyber suggested going for individual certifications for each customer's environment and multi-tenant platform.

Environment Overview

The assessment covered two primary categories of environments:

1. **Primary Multi-Tenant Platform:**
   - Hosted over 30 banking applications and associated services.
   - Deployed across AWS and Azure cloud infrastructure.
   - Served multiple financial institutions through a shared infrastructure model.
   - Implemented advanced security controls to ensure tenant isolation.

2. **Dedicated Customer Bank/Regional Environments:**
   - Individual environments require separate certification.
   - Distributed across multiple cloud providers (AWS, GCP, Azure, Raya Cloud, Oman Data Park, Oracle Cloud).
   - Customized to meet specific requirements of each financial institution.
   - Varying architectural patterns and security controls.

All environments utilized modern cloud-native technologies including containerization via Kubernetes, serverless computing models, and infrastructure automation through Terraform, presenting unique challenges for PCI DSS compliance assessment.

Assessment Methodology and Execution

The gap assessment phase was conducted on-site over a three-week period. Ampcus Cyber's assessment team performed detailed technical reviews of each environment, examining both infrastructure components and application layers. The assessment methodology included:

01 Comprehensive documentation review.

02 Interviews with key personnel.

03 Configuration analysis of cloud environments.

04 Security control testing.

05 Segmentation verification.

Due to the interconnected nature and complexity of the environments, the team implemented a systematic approach where any identified issues were cross-verified across all environments to ensure consistent remediation. This approach was particularly important given the multi-cloud architecture and the use of diverse deployment technologies.

Remediation Support and Certification

Following the gap assessment, Ampcus Cyber worked closely with the organization to address all identified findings. The remediation support included:

01 Detailed guidance on required controls.

02 Technical assistance for complex implementation challenges.

03 Validation testing of implemented solutions.

04 Cross-environment verification of remediation effectiveness.

This collaborative approach enabled the organization to successfully implement all required controls across their complex cloud environments within the established timeline. The final certification was completed on schedule, demonstrating the effectiveness of both the assessment methodology and the subsequent remediation efforts.

Conclusion

This assessment represented a particularly complex PCI DSS certification engagement due to the multi-tenant architecture, diverse cloud platforms, and advanced deployment technologies involved. Through methodical execution and close collaboration, Ampcus Cyber successfully guided the organization through the certification process, ensuring all environments met the stringent requirements of the PCI DSS standard.