



CUSTOMER SUCCESS STORY

SISA's consultative approach helped a Banking major ease PCI compliance journey and improve security posture

ABOUT THE CUSTOMER



The client is a leading Bank in the GCC region with 66 branches and 400+ ATMs/CDMs in the United Arab Emirates (UAE) and holding >30% market share among UAE banks (by assets). Headquartered in Abu Dhabi, the bank's international network spans 19 markets across five continents serving more than 3 million customers. As one of the largest regional banks, it offers an extensive range of solutions and services across consumer banking, private banking, investment banking and corporate banking. With a strong focus on technology and sustainability, the bank is also a recipient of several prestigious awards such as the Safest Bank in the UAE by Global Finance and The Most Innovative Investment Bank from the Middle East by The Banker.

THE CHALLENGE

The bank was keen to achieve PCI-DSS compliance – one of the most stringent and coveted security standards with 12 requirements and over 300 sub-requirements for the cardholder data environment. The requirement was primarily born out of CBUAE's regulatory mandate, but the bank faced implementation challenges on multiple fronts.

- Firstly, being a maiden compliance exercise, the lack of clear and well-defined processes created operational roadblocks.
- Next, a diverse technology landscape and the high level of application dependency coupled with end of life (EOL) systems added to the complexity of the organization's infrastructure. All the endpoint systems had hit EOL operating systems (OS) and some of the file servers, DB servers and app servers were using outdated OS.
- Thirdly, the bank's environment spanning 1,000+ servers, 2,000+ endpoints and 100+ databases, was complex and vast. The extensive infrastructure landscape – a consequence of the merger executed previously and the merged entity's subsequent diversification into a new business line, expanded the scope of the assessment.





SOLUTION OFFERED BY SISA

SISA kicked off the engagement by conducting a “Certified Payment Card Industry Security Implementer” (CPISI) in-house workshop for the bank’s 35-member team of senior executives. This helped the bank bridge the awareness gap and improve their preparedness for implementing PCI security controls. In parallel, SISA also created a policy and procedure document to help ease the compliance journey. Thereafter, SISA proposed a three-phased approach to implementation consisting of Scoping and Assessment, Remediation and Certification.

SISA assessed the bank's business critical data spread across its environment and found that the cardholder data was stored in multiple databases in plain text. Other major lapses were uncovered such as non-deployment of file integrity monitoring solution and non-integration of application logs and audit trails for servers with SIEM solution. To help the bank address these, SISA recommended 200+ action points for remediation such as MFA controls, password management policy, cardholder data retention and disposal policy and advised the bank to perform vulnerability scans and penetration testing. To address the challenge of a large-scale environment, SISA segregated the remediation actions under three milestones and mapped these to their respective departments. This enabled the bank to close the security gaps within the planned schedule.

BUSINESS IMPACT

By investing in relevant security tools and remediating all the action points recommended by SISA, the bank was successful in achieving PCI-DSS certification in six months’ time. SISA’s in-house training and multi-phased assessment offered the bank a window to meet PCI-DSS compliance standards across its Issuing, ATM acquiring and banking services (including Conventional, Islamic and HNI) for the UAE market. In addition, the certification also helped the bank achieve a better security posture and comply with regulatory mandates along with improving trust among its customers.

A forensics driven cybersecurity company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

PCI Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audits

Security Testing

Application Security

- Application
- Penetration Testing
- CREST/CERT-in Approved
- Security Testing
- API Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Detection and Response Solution

SISA ProACT

Incident Response and Forensics

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool - SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs

- CIDR

Forensic Learning Sessions for Senior Management