



CUSTOMER SUCCESS STORY

SISA's training-led multi-phase assessment helps legacy bank successfully achieve PCI DSS compliance



ABOUT THE CUSTOMER

As one of the largest banks in Bangladesh, BRAC Bank was established in 2001 with a vision of building a financial ecosystem that contributes to a more democratic and poverty-free country. Headquartered in Dhaka, the bank serves more than 1.3 million retail, corporate, and SME business customers through a variety of channels, including a growing portfolio of customer-centric digital products. It has a nationwide presence spanning 187

branches, 461 SME offices, 375 ATMs, 730 Agent Banking Outlets and 96 CDMs. Besides, as an issuer and acquiring bank, it offers credit, debit, and prepaid cards while also handling POS transactions. Approximately half of the bank's lending portfolio comprises small and medium enterprises – reflecting its vision of providing banking solutions to the 'unbanked' SMEs.



THE CHALLENGE

In a quest to reform the country's banking sector and strengthen the security posture, the Central Bank of Bangladesh issued an order mandating PCI DSS compliance for all banks by the end of December 2019. But BRAC Bank started the PCI-DSS journey in 2016. During the PCI-DSS journey, the bank faced multiple challenges. The first was to create internal awareness on the importance of PCI DSS implementation

across the bank. Secondly, the bank needed to start the process from scratch as it did not have access to the necessary tools required to comply with PCI DSS requirements. Thirdly, as a second-generation bank with heavy legacy infrastructure, it had to upgrade multiple solutions including several in-house applications running into a multi-year effort.

"As part of our commitment to protect customers' interests, BRAC Bank has embraced the Compliance Standard diligently, establishing compliance and setting risk assessment frameworks. PCI DSS Certification shows the bank's strong commitment to safeguarding information and interests of the customers. We think it will give the customers confidence to safely bank with us."

Md. Sabbir Hossain, Deputy Managing Director & COO

SOLUTION OFFERED BY SISA

As a first step, SISA conducted a Certified Payment Card Industry Security Implementer (CPI SI) in-house workshop for the bank's senior executives. This helped the bank gain a broad understanding of the implementation process and the consequent benefits. As a next step, the bank sought SISA's assistance in securing its information systems in line with global industry standards. SISA assessed the bank's business-critical data spread across its environment and found that the cardholder data was stored in multiple databases, backups, logs, etc. in plain text. Further, there were 17 applications that generated reports containing full card number that was visible to the team. SISA recommended the use of multi-level encryption and strong key management along with a policy for sending encrypted PAN via end-user messaging technologies.

The bank was also performing the upload, download, and deletion of embossing files

manually which resulted in the storage of PAN details in local systems. SISA provided detailed guidance on how to minimize the manual intervention and suggested automating these processes. Although the bank had performed VAPT, there were gaps in performance and the scope was restricted to servers and critical applications only. To overcome this, SISA helped in setting up the process to cover the complete scope and listed out detailed procedures for network PT and segmentation PT, following which the bank procured multiple licensed tools to fulfil this requirement. Additionally, SISA created end-to-end cardholder data flow diagram for the issuing process to aid in compliance preparation for other processes. SISA also helped the bank perform the cardholder data scan (using the third-party tool) on a quarterly basis and purge the data post retention.

"This certification means BRAC Bank is a place where customer information is unassailably safe and secured leaving no vulnerability to data theft and loss. This is just the beginning of our partnership with SISA, which we believe will reach new level with more mutual collaboration in the coming years."

B. M. Zahid-ul Haque, Head of Information Security

BUSINESS IMPACT

By investing in relevant security tools, conducting several security assessments and multiple pieces of training, and remediating all the action points recommended by SISA, the bank was successful in achieving PCI-DSS certification. It also conferred on the organization the privilege of being one of the only three scheduled commercial banks

in the country to be PCI-DSS certified. In this process, the bank upgraded its eCommerce Platform, credit card solution, payment switch system, CORPnet, internet banking system, and core banking system enabling it to offer complete data protection to customers. The bank has also established 24x7 Security Operations Centre.

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