

# searchSecurity.in

## PCI-DSS standard compliance becomes reality for Bank of India

Although the [payment card industry data security standard \(PCI-DSS\)](#) is not yet mandated by Reserve Bank of India, Indian banks are already keen on acquiring the certification. Leading public sector bank – Bank of India – recently achieved PCI-DSS standard compliance for its debit card environment, and claims to be the first Indian bank to do so.

Bank of India has to deal with critical debit card data of thousands of its customers. The bank recently moved the debit card automated teller machine switches — the authentication server and interface components — to its own data center, compelling it to have an additional layer of security. “Although there was no direct mandate, we felt that [adopting the PCI-DSS standard](#) on top of ISO 27001 would help us strengthen our security posture,” says Sameer Ratolikar, the chief information security officer at Bank of India.

### More stories on PCI-DSS compliance

[PCI DSS certification: Three myths that affect its success in India](#)

[PCI-DSS compliance best practices](#)

[PCI DSS certification boosts customer confidence at Zenta](#)

[Hectic race to meet Visa's PCI-DSS compliance deadline](#)

### Gap analysis process

To obtain the [PCI-DSS standard certification](#), Bank of India announced an expression of interest (EOI) from security vendors, analyzed their presentations, and floated a tender. The bank called for technical as well as price bids and after a thorough analysis based on the lowest bidder criteria, selected Bangalore-based SISA as its consultant. CERT-In empanelment was one of the most important criteria at this stage (CERT-IN shortlists a security company as its member through a very rigorous process). The bank also checked if SISA had ever been blacklisted or the PCI-DSS certification of any of its earlier customers was revoked.

SISA was involved as a consultant right from the Gap analysis stage. SISA advised the bank to form a core team comprising managers from its zonal, regional and branch offices, as well as members from its database, application, network, infrastructure, data center, IT and risk management teams. The Gap analysis process took around a month, after which the bank started the mitigation process.

All the 12 [requirements of PCI-DSS standard](#) were applicable to Bank of India. Of these, Ratolikar found ‘protection of card holder data’ as one of the toughest requirements to comply with. As Ratolikar observes, “Data protection goes beyond data security and also includes protection of personal identifiable information and indirect mapping to section 43A of IT Amendment Act 2008.” The bank had to ensure that all kinds of data, that is, data at rest (saved in databases), data in motion (emails and other communication) and data in process were protected. To ensure this, the bank uses its Microsoft’s digital rights management solution (implemented prior to the PCI-DSS project). Bank of India also conducts vulnerability assessment and penetration testing (through and external vendor and internal team) on all assets carrying the debit card data in every quarter as part of [PCI-DSS standard’s scope](#). The bank uses a layered approach comprising various technical controls like firewalls, intrusion prevention system, and log monitoring using security information and event management to ensure complete data protection.

## Combating key issues

After the Gap analysis, the bank found certain issues related to router level configuration, storage of data in application, and its transmission between branches, regional, and head offices. “For instance, the transmission of debit card data earlier took place in the plain text. Now at the enterprise level, we have advised people to zip the data and make it password protected,” explains Ratolikar. The bank currently uses 7 zip and WinZip 11 for encryption and plans to procure dedicated software to encrypt all communication dealing with debit card data.

Before [adopting the PCI-DSS standard](#), Bank of India’s internet banking database did not store debit card numbers in the encrypted format, as required. Now, it stores only truncated card numbers, saving the first six and last four digits. SISA also reviewed the bank’s information security (IS) framework and suggested changes in its access control policy, segregation of roles and responsibilities, application, and database security. The bank implemented these changes and got it approved from its board.

[Ensuring PCI-DSS standard](#) compliance at the branch level was the biggest challenge, as the bank did not have enough technical manpower. Hence, it took help from zonal offices, where the IT officers regularly visited the branches and sensitized branch staff about [PCI-DSS standard requirements](#) “We also used our e-learning tool – Star Live – to conduct training awareness sessions for the branch staff,” adds Ratolikar.

## Reaping the benefits

Bank of India’s PCI-DSS project incurred a cost of Rs 10 lakh, and was executed in six months. Being ISO 27001 compliant, the bank already had sufficient IS controls and processes and hence, did not require any additional technology.

[PCI-DSS standard compliance](#) has helped Bank of India create an IS culture across the organization, enabling it to take employee awareness to the next level. In future, the bank plans to ensure merchant compliance under PCI-DSS standard.

All Rights Reserved, [Copyright 2009 - 2010](#), TechTarget | [Read our Privacy Statement](#)