

Structured Approach to Multi-Location PCI DSS Compliance for Better Time Management



Snapshot

Client Industry: BPO

Global Locations: approx. 117

Number of Processes: 70

Compliance Duration: approx. 4 months

Challenge: Efficiently achieving PCI compliance across multiple geographies

Solution: Structured approach to organization-wide compliance certification

Benefits: Quicker PCI DSS Certification process and improved security posture

Multiple Locations, Multiple Certifications

For organizations that operate out of multiple locations around the globe, maintenance of a uniform PCI Calendar is a tough task. This gets even trickier when there are mergers/acquisitions involved, since each sub-location is likely to follow its own set of policies, procedures, technologies, security architecture, etc. and this consumes more time.

They are also likely to have different PCI certification timelines. Unless these are consolidated and brought onto a single schedule, the organization's InfoSec team has to spend additional time to achieve certification. They will need to perform compliance, assessment, and auditing activities for each location following their unique schedule, throughout the year. Through consolidation, the company can save the overall cost and the hassle of putting greater amounts of human effort, which can be redirected to other areas of concern and security related upgradations.

One of the top BPO companies, headquartered in India was facing a similar issue every time, when it went for PCI DSS compliance for the parent company as well as its subsidiaries (some of which, were acquired) across the globe. The company was keen to have a single PCI DSS calendar for all its location to strengthen security, save time, and bring efficiency.

One Company, One Certification, One Schedule

The first step for SISA was to gain a thorough understanding of the client's environment. For this, the QSA did the necessary groundwork to know the business and security processes, by visiting the company's headquarters and meeting its top management and CISO.

SISA then recommended the company to consolidate all its PCI certification efforts, across locations into a single process. It conducted in-house training on PCI DSS to educate the company's associates on the benefits of merging two different entities (spread across multiple locations) into one. The company understood the advantages of doing this and agreed to go ahead with the solution offered.

SISA then helped the company to follow a structured approach by doing an organization-wide certification process. As part of this, the PCI audit was conducted for all the locations again, even though some of them had been recently certified. This was important in order to bring all the subsidiaries onto a single timeframe for future audits.

An assessment on the scope was conducted to determine the number of desktops and processes within the organization that dealt with business critical data, as well as the locations that were set up to handle this data. Once the scoping was completed, an ROC certificate was issued. This was done both through onsite assessment and sampling of the regions with higher number of PCI DSS processes.

“ We were able to achieve compliance across all our locations with minimal time and effort. This milestone was achieved by the company with great coordination, trust, and support of the higher management, the CISO, and the SISA team. ”

For any entity that is spread across regions, having a centralized control is suggested to ease security monitoring. Alternately, having region-wide controls is a must. Therefore, path management can be conducted at regional and centralized locations without any overlap of times.

Comprehensive System and Efficient Process

The exercise resulted in overall time savings for the organization, as it gave an ability to complete the PCI DSS compliance process for the whole entity at once, bringing all the certifications together. This in turn benefitted them with freed up time and resources to focus on other types of certifications such as ISO 27001, SOX, and HIPAA.

Also, the team was able to get greater visibility into its scope of requirements and gain a better security posture.

Reach us at sales@sisainfosec.com