PCI DSS COMPLIANCE PROCEDURE

How to secure sensitive card data with PCI Data Security Standard (PCI DSS)

It is crucial to attain and preserve compliance so that the organization's cyber security is appropriately and efficiently protected against cybercriminals aiming to steal card information.

The payment brands have agreed to include the PCI Data Security Standards as a component of the technical requirements for each of their data security compliance programs. The 5 brands will also accept validation when it is recognized by security assessors themselves or approved scanning vendors, parties qualified by the PCI Security Standards Council.

Hence, as a first step to obtain information on how to become and maintain its PCI DSS compliance, we recommend that you contact your acquirer.

If you do not have an acquirer, we suggest that you contact the bank's branch that you are working with.

PCI Data Security Standard Requirements

ASSESS

Goal: Taking the inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data.

Assessment is responsible for recognizing all the possible issues which would translate into a risk for the security of the cardholder data that is being transmitted, processed or stored by your business. By further reading the information on the PCI DSS website, you can understand more about the detailed requirements, related to the infrastructure and several processes involved into the whole transaction process.

It is important to note that the third parties involved in your compliance process, are compliant also. A thorough assessment will help in the full comprehension of all possible vulnerabilities and places where remedying will be needed.

The Self- Assessment Questionnaire (SAQ)
The SAQ is a validation tool for eligible merchants and service providers who self-evaluate their PCI DSS compliance.

Qualified Assessors
The Council Provides programs for two kinds of independent experts to help with your PCI assessment: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to asses and prove compliance with PCI DSS. ASVs provide commercial software tools and analysis services for performing external vulnerability scans for your system. The PCI SSC also provides educational resources for merchants and service providers, including training for Internal Security Assessors (ISAs).

REMEDIATE

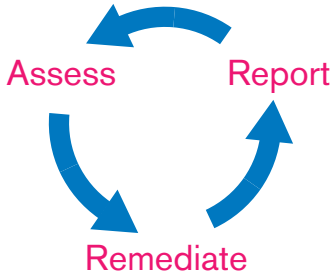
Goal: The process of fixing vulnerabilities.

Scanning your network with software tools that analyze infrastructure and spot known vulnerabilities
Review and remediation of vulnerabilities found in on-site assessment (if applicable) or through the self-assessment process
Classifying and ranking the vulnerabilities to help prioritize the order of remediation
Applying patches, fixes, workarounds, and changes to unsafe processes and workflow
Re-scanning to verify that remediation actually occurred

REPORT

Goal: The compilation of records required by PCI DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands you do business with.

Regular reports are required for PCI DSS compliance; these are submitted to the acquiring bank and payment card brands that you do business with. PCI SSC is not responsible for enforcing PCI DSS compliance. All merchants, service providers and processors may be required to submit quarterly scan reports, which must be performed by a PCI SSC approved ASV. Businesses with smaller transaction volumes may be required to submit an annual Attestation within the Self-Assessment Questionnaire. For more details on validation and reporting requirements, speak with your acquirer or payment card brand.



Source: Getting started with PCI DSS
If you have any questions, please refer to our FAQs