The intent of this PCI DSS Quick Reference Guide is to help you understand how the PCI DSS can help protect your payment card transaction environment and how to apply it.

There are three ongoing steps for adhering to the PCI DSS:

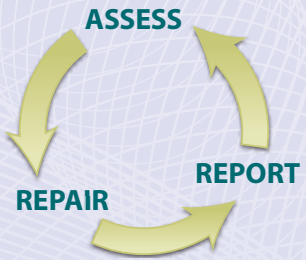
Assess — identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.

Repair — fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.

Report — documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands you do business with (or other requesting entity if you're a service provider).

PCI DSS follows common-sense steps that mirror security best practices. The PCI DSS globally applies to *all* entities that store, process or transmit cardholder data and/or sensitive authentication data. PCI DSS and related security standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Participating Organizations include merchants, payment card issuing banks, processors, developers and other vendors.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.