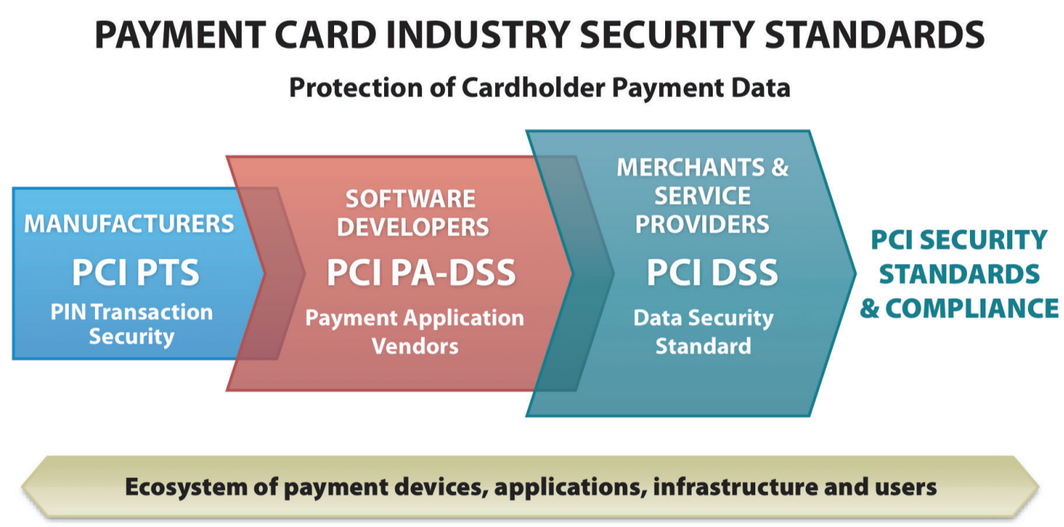
PCI-DATA SECURITY STANDARD (DSS) CONTROLS

PCI Security Standards Council

OVERVIEW

PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.



PCI DATA SECURITY STANDARD (DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

PCI-DDS CONTROLS

1: Protect Your System with Firewalls	2: Configure Passwords and Settings	3: Protect Stored Cardholder Data
4: Encrypt Transmission of Cardholder Data Across Open, Public Networks	5: Use & Regularly Update Anti-Virus Software	6: Regularly Update and Patch Systems
7: Restrict Access to Cardholder Data by Business	8: Assign a Unique ID to Each Person with Computer Access	9: Restrict Physical Access to Workplace and Cardholder Data
10: Implement Logging and Log Management	11: Conduct Vulnerability Scans and Penetration Tests	12: Documentation and Risk Assessments

NSF NCYTE CENTER PCI Security Standards Council™ CSSIA National Resource Center for Systems Security and Information Assurance