

PCI DSS Roadmap

ver1.0TECsgSF

The 12 PCI DSS requirements are organized into 6 main categories. To be fully compliant, an organization must satisfy all 12 requirements.

- *Maintain a Secure Network: Requirements 1 and 2*
 - Install and maintain a firewall configuration to protect cardholder data
 - Do not use vendor-supplied defaults for system passwords and other security parameters
- *Protect Cardholder Data: Requirements 3 and 4*
 - Protect stored cardholder data
 - Encrypt transmission of cardholder data across open, public networks
- *Maintain a Vulnerability Management Program: Requirements 5 and 6*
 - Use and regularly update anti-virus software
 - Develop and maintain secure systems and applications
- *Implement Strong Access Controls: Requirements 7, 8, and 9*
 - Restrict access to cardholder data by business need-to-know
 - Assign a unique ID to each person with computer access
 - Restrict physical access to cardholder data
- *Regularly Monitor and Test Networks: Requirements 10 and 11*
 - Track and monitor all access to network resources and cardholder data
 - Regularly test security systems and processes
- *Maintain an Information Security Policy: Requirement 12*
 - Maintain a policy that addresses information security

<http://www.PCISecurityStandards.org>.