PCI DSS

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

SC
Cyber Solutions

PCI DSS

- Payment Car Industry Data Security Standard
- Developed due to increase in identity theft, credit card fraud
- Set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express
- Has a set of requirements for credit card and debit card transactions and account data security
- Latest version – v4.0 – released March 2022

shweta@sccybersolutions.com

SC
Cyber Solutions

- Governed by the Payment Card Industry Security Standards Council (PCI SSC)
- PCI SSC has no legal authority to compel compliance
- It is a requirement for any business that processes credit or debit card transactions

shweta@sccybersolutions.com

SC
Cyber Solutions

Who has to comply

- Merchants
- Service providers

shweta@sccybersolutions.com

SC
Cyber Solutions

Compliance Levels

- PCI compliance is divided into four levels, based on the annual number of credit or debit card transactions a business processes

shweta@sccybersolutions.com

SC
Cyber Solutions

- Level 1
  - Internal audit conducted by an authorised PCI auditor annually
  - Quarterly PCI scan by an Approved Scanning Vendor (ASV)

- Level 2
  - Complete an assessment once a year using a Self-Assessment Questionnaire (SAQ)
  - Quarterly PCI scan by an Approved Scanning Vendor (ASV) might be needed

shweta@sccybersolutions.com

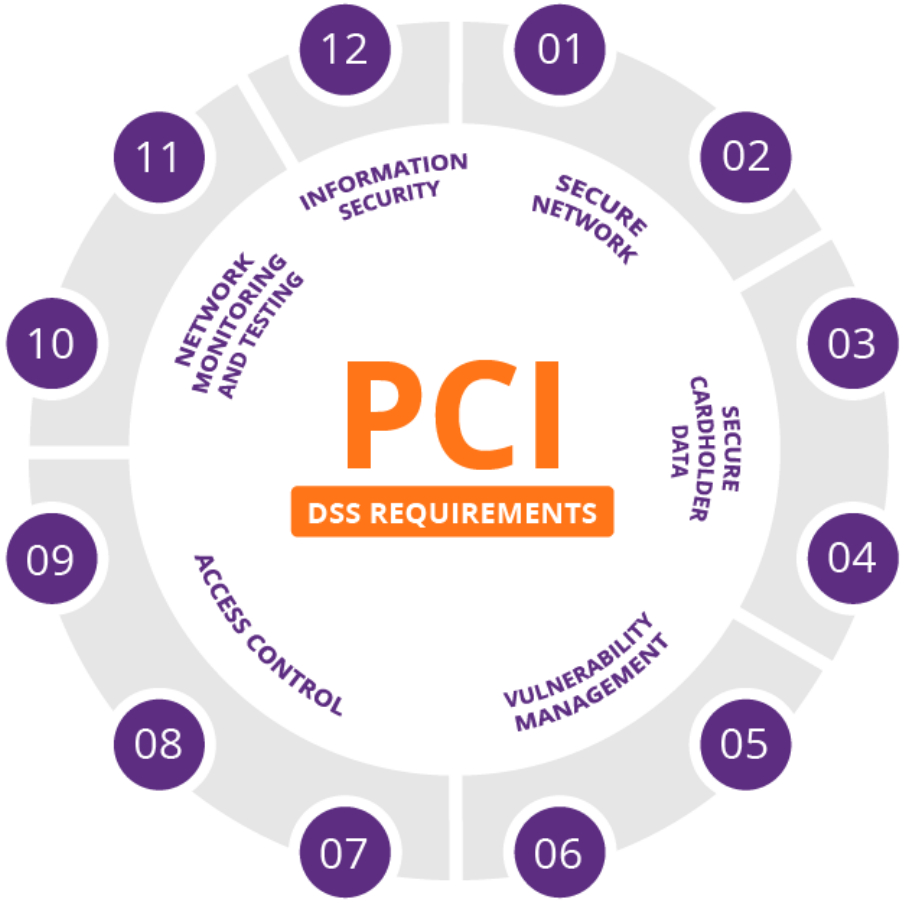
- Level 3
  - Complete an assessment once a year using a Self-Assessment Questionnaire (SAQ)
  - Quarterly PCI scan by an Approved Scanning Vendor (ASV) might be needed

- Level 4
  - Complete an assessment once a year using a Self-Assessment Questionnaire (SAQ)
  - Quarterly PCI scan by an Approved Scanning Vendor (ASV) might be needed

shweta@sccybersolutions.com

SC
Cyber Solutions

Requirements



shweta@sccybersolutions.com

SC
Cyber Solutions

- Secure network
  - A firewall configuration must be installed and maintained
  - System passwords must be original (not vendor-supplied)
- Secure cardholder data
  - Stored cardholder data must be protected
  - Transmissions of cardholder data across public networks must be encrypted
- Vulnerability management
  - Anti-virus software must be used and regularly updated
  - Secure systems and applications must be developed and maintained

shweta@sccybersolutions.com

SC
Cyber Solutions

- Access control
  - Cardholder data access must be restricted to a business need-to-know basis
  - Every person with computer access must be assigned a unique ID
  - Physical access to cardholder data must be restricted
- Network monitoring and testing
  - Access to cardholder data and network resources must be tracked and monitored
  - Security systems and processes must be regularly tested
- Information security
  - A policy dealing with information security must be maintained

shweta@sccybersolutions.com

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300