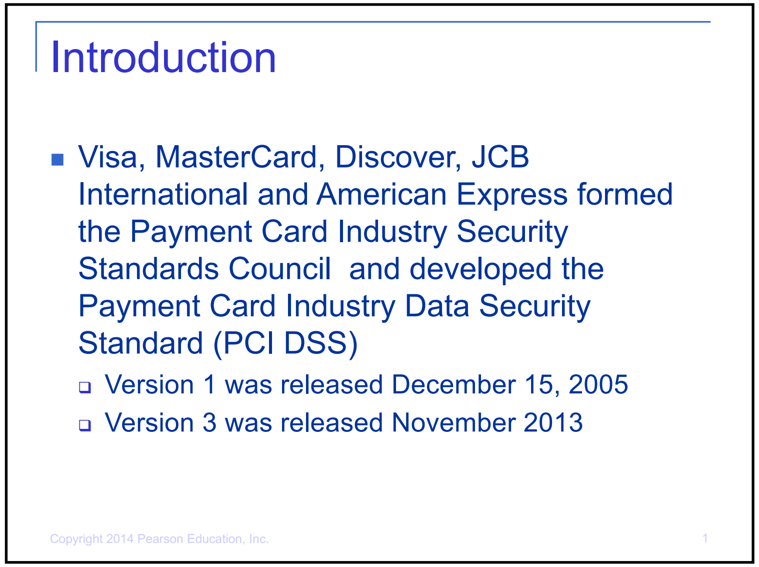
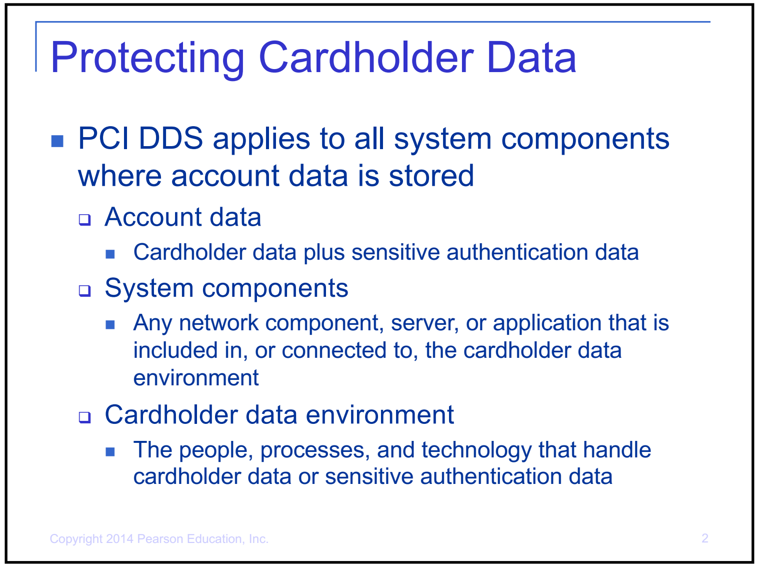


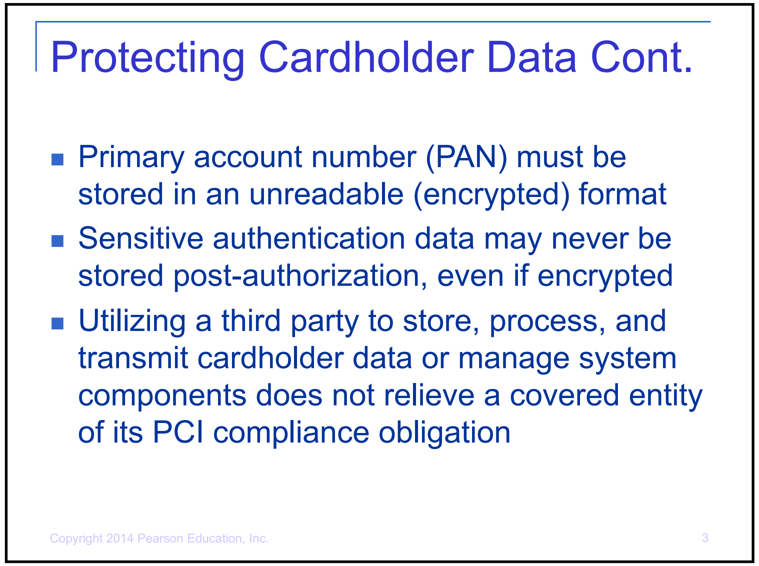
Introduction

- Visa, MasterCard, Discover, JCB International and American Express formed the Payment Card Industry Security Standards Council and developed the Payment Card Industry Data Security Standard (PCI DSS)
  - Version 1 was released December 15, 2005
  - Version 3 was released November 2013



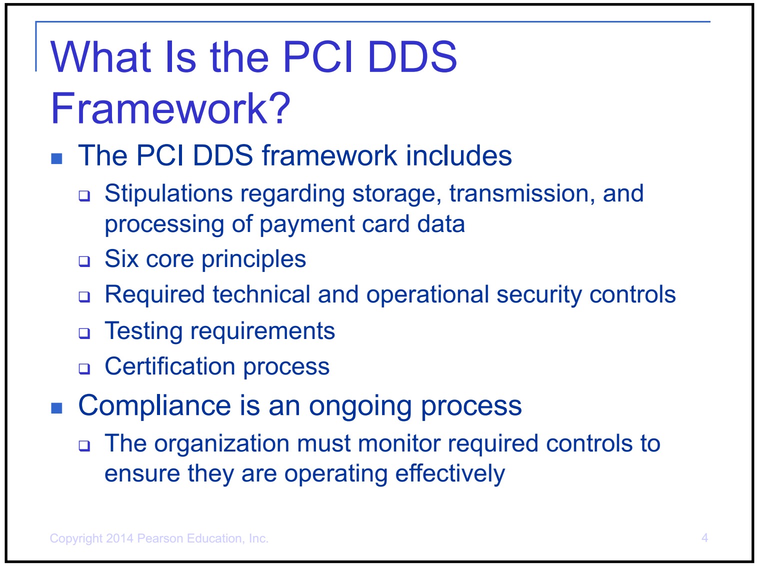
Protecting Cardholder Data

- PCI DDS applies to all system components where account data is stored
  - Account data
    - Cardholder data plus sensitive authentication data
  - System components
    - Any network component, server, or application that is included in, or connected to, the cardholder data environment
  - Cardholder data environment
    - The people, processes, and technology that handle cardholder data or sensitive authentication data



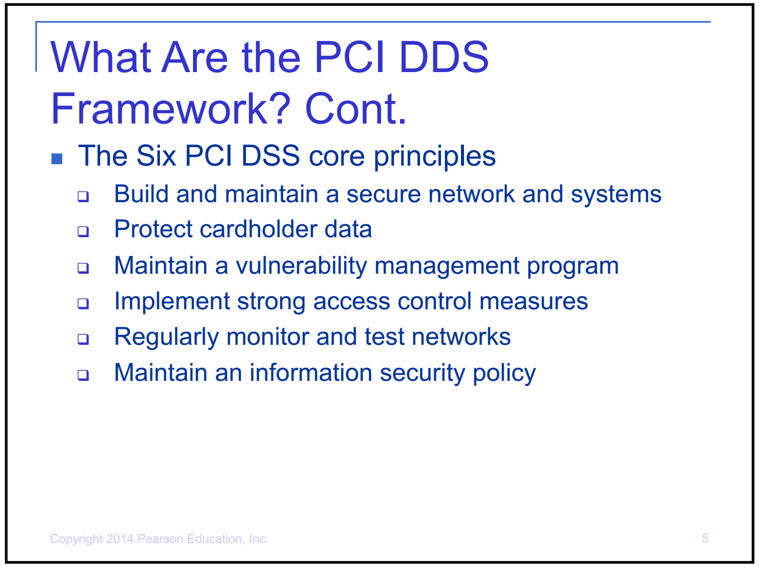
Protecting Cardholder Data Cont.

- Primary account number (PAN) must be stored in an unreadable (encrypted) format
- Sensitive authentication data may never be stored post-authorization, even if encrypted
- Utilizing a third party to store, process, and transmit cardholder data or manage system components does not relieve a covered entity of its PCI compliance obligation



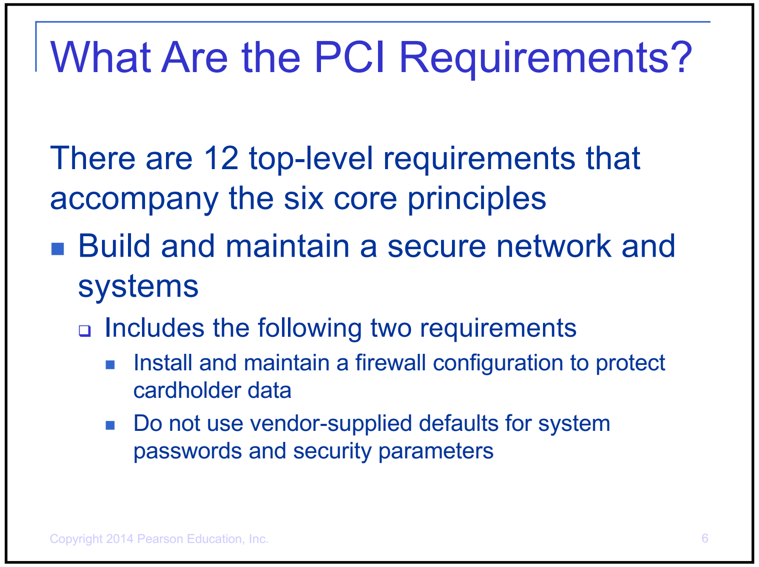
What Is the PCI DDS Framework?

- The PCI DDS framework includes
  - Stipulations regarding storage, transmission, and processing of payment card data
  - Six core principles
  - Required technical and operational security controls
  - Testing requirements
  - Certification process
- Compliance is an ongoing process
  - The organization must monitor required controls to ensure they are operating effectively



What Are the PCI DDS Framework? Cont.

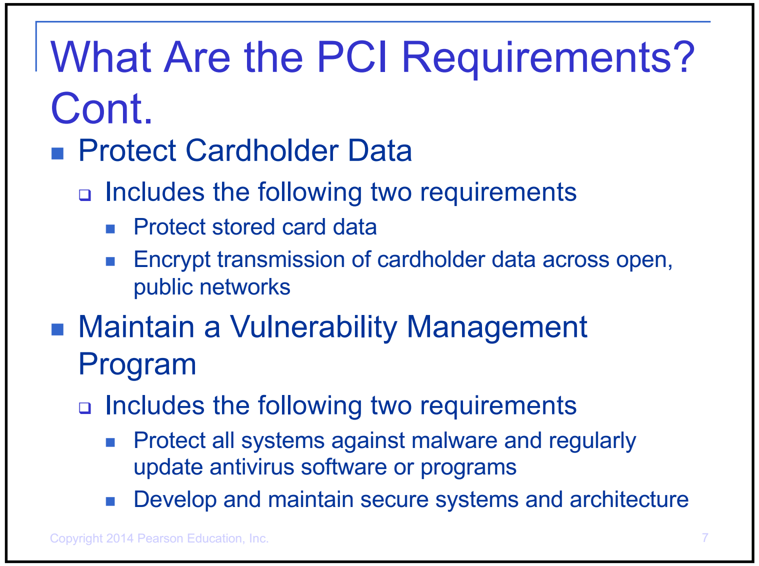
- The Six PCI DSS core principles
  - Build and maintain a secure network and systems
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy



What Are the PCI Requirements?

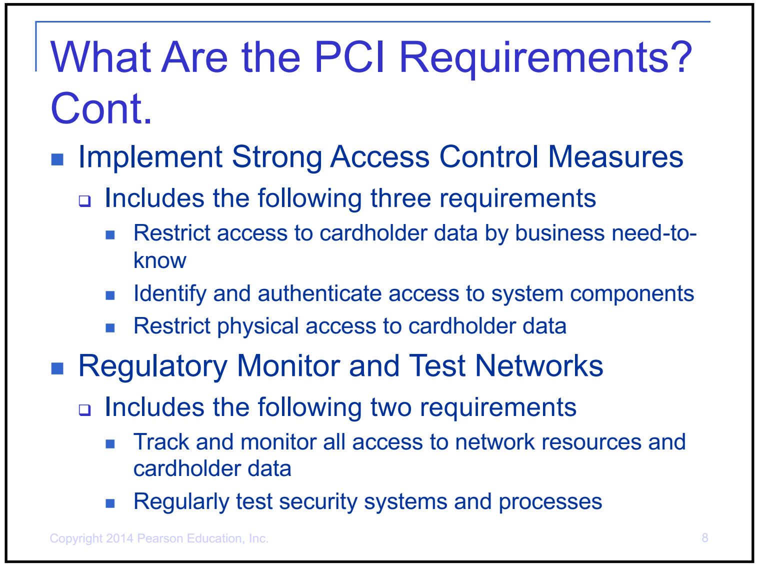
There are 12 top-level requirements that accompany the six core principles

- Build and maintain a secure network and systems
  - Includes the following two requirements
    - Install and maintain a firewall configuration to protect cardholder data
    - Do not use vendor-supplied defaults for system passwords and security parameters



What Are the PCI Requirements? Cont.

- Protect Cardholder Data
  - Includes the following two requirements
    - Protect stored card data
    - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Includes the following two requirements
    - Protect all systems against malware and regularly update antivirus software or programs
    - Develop and maintain secure systems and architecture



What Are the PCI Requirements? Cont.

- Implement Strong Access Control Measures
  - Includes the following three requirements
    - Restrict access to cardholder data by business need-to-know
    - Identify and authenticate access to system components
    - Restrict physical access to cardholder data
- Regulatory Monitor and Test Networks
  - Includes the following two requirements
    - Track and monitor all access to network resources and cardholder data
    - Regularly test security systems and processes

What Are the PCI Requirements? Cont.

- Maintain an Information Security Policy
  - Includes the final requirement
    - Maintain a policy that addresses information security for all personnel

PCI Compliance

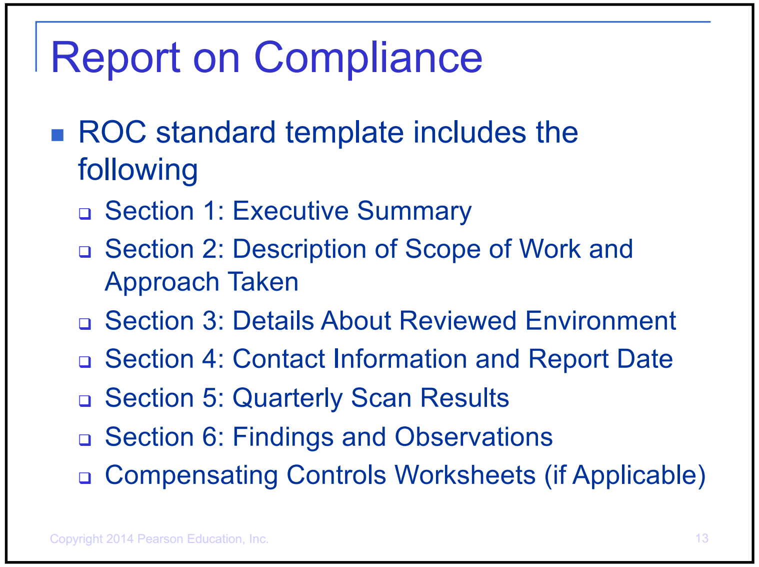
- PCI compliance is not a government regulation or law
- It’s mandated by the payment card brands to accept card payments and/or be part of the payment system
- Merchants are required to comply with PCI DSS
  - A merchant is defined as any entity that accepts American Express, Discover, JCB, MasterCard, or Visa payment cards as payment for goods and/or services (including donations)
  - Effectively, any company, organization, or individual that accepts card payments is a merchant

PCI Compliance Cont.

- PCI compliance validation is composed of four levels, based on the number of transactions processed per year and whether those transactions are performed from a physical location or over the Internet
  - Level 1
    - Processes more than 6 million Visa payment card transactions annually
  - Level 2
    - Processing 1million to 6million Visa transactions per year.
  - Level 3
    - Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year
  - Level 4
    - Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel—processing up to 1million Visa transactions per year

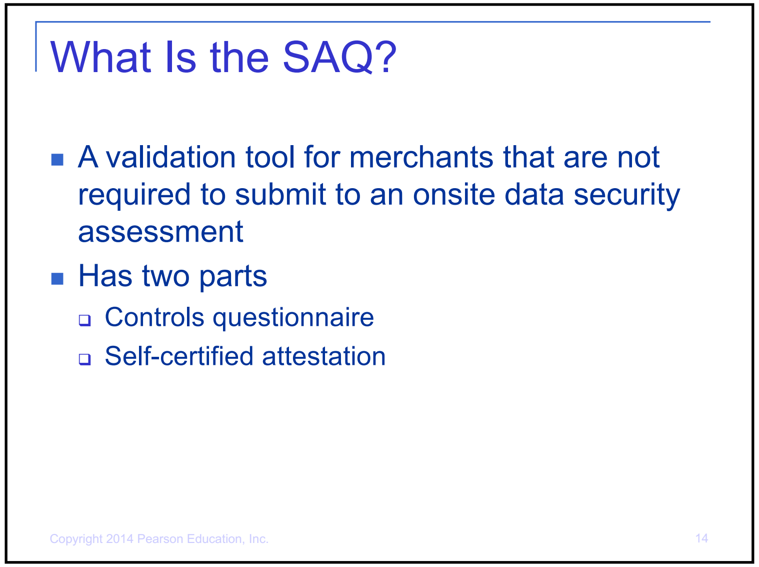
What Is a Data Security Compliance Assessment?

- An annual onsite evaluation of compliance with the PCI DSS conducted by either a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA)
- Assessment process begins with documenting the PCI DSS cardholder environment and confirming the scope of the assessment
- QSA/ISA will initially conduct a GAP assessment to identify areas of noncompliance and provide remediation recommendations



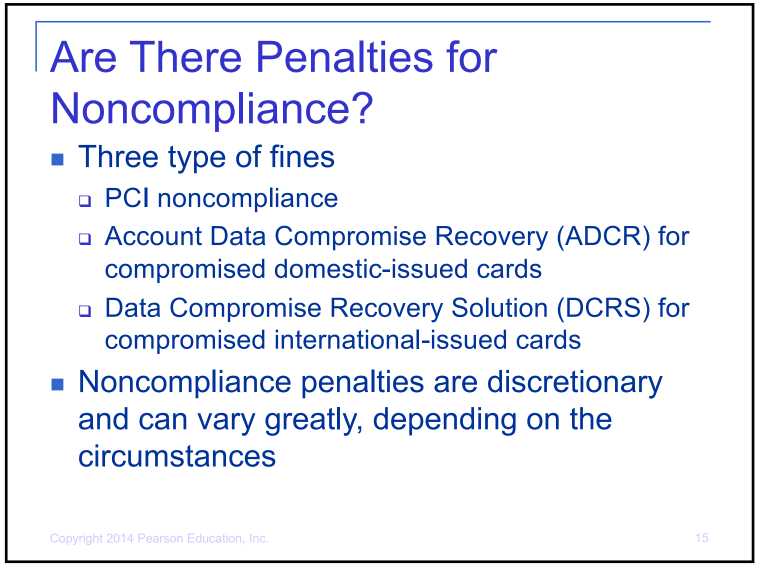
Report on Compliance

- ROC standard template includes the following
  - Section 1: Executive Summary
  - Section 2: Description of Scope of Work and Approach Taken
  - Section 3: Details About Reviewed Environment
  - Section 4: Contact Information and Report Date
  - Section 5: Quarterly Scan Results
  - Section 6: Findings and Observations
  - Compensating Controls Worksheets (if Applicable)



What Is the SAQ?

- A validation tool for merchants that are not required to submit to an onsite data security assessment
- Has two parts
  - Controls questionnaire
  - Self-certified attestation



Are There Penalties for Noncompliance?

- Three type of fines
  - PCI noncompliance
  - Account Data Compromise Recovery (ADCR) for compromised domestic-issued cards
  - Data Compromise Recovery Solution (DCRS) for compromised international-issued cards
- Noncompliance penalties are discretionary and can vary greatly, depending on the circumstances