Security Strategies in Web Applications and Social Networking

Lesson 10

Maintaining PCI DSS Compliance for E-commerce Web Sites

Learning Objective and Key Concepts

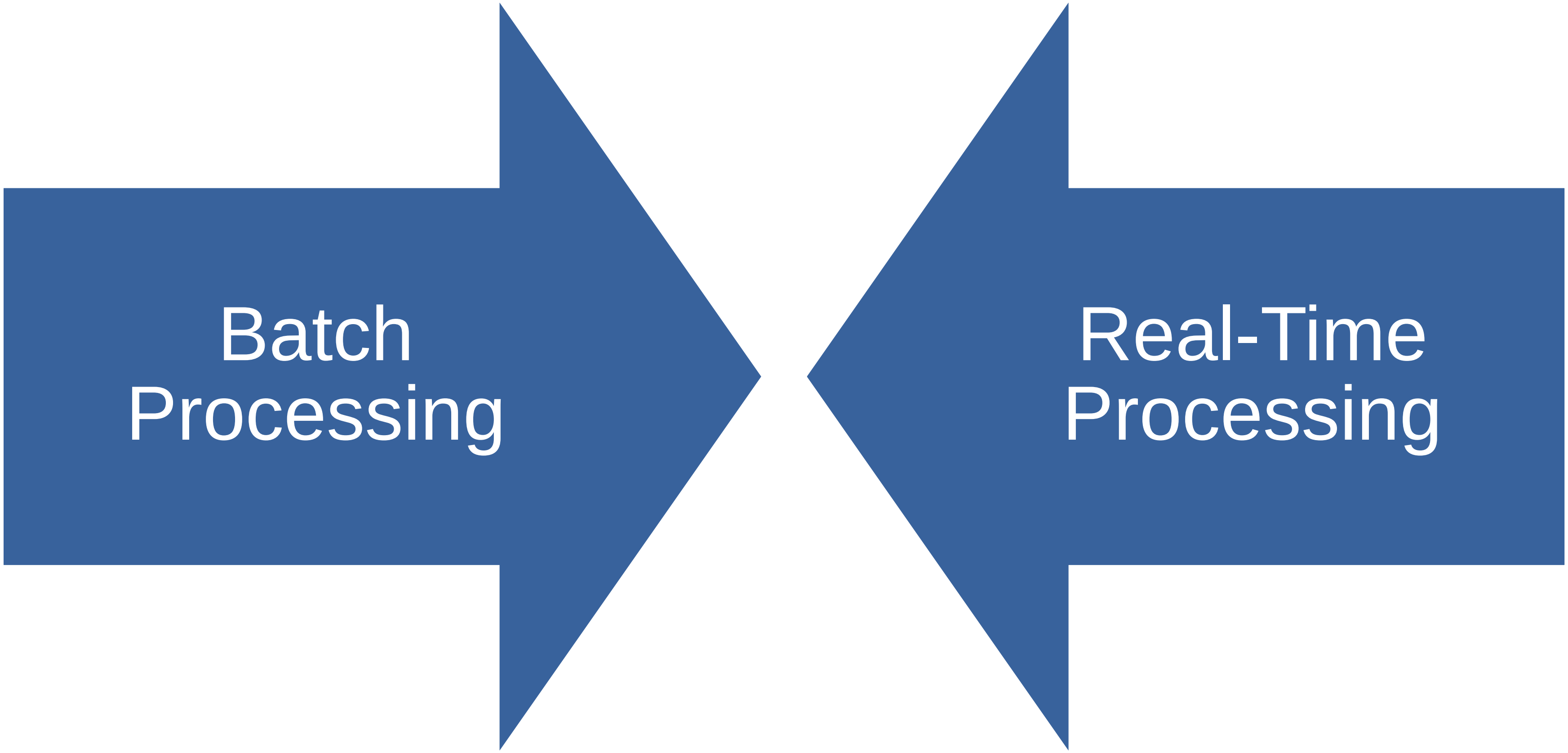
Learning Objective

- Analyze the role and importance of audit and compliance to Web application security.

Key Concepts

- Audit and compliance obligations
- Consequences for noncompliance
- The Payment Card Industry Data Security Standard (PCI DSS)
- Public and private sector regulations

Credit Card Transaction Processing



Batch Processing

Real-Time Processing

PCI DSS

- A set of widely accepted standards for securing credit card data
- Developed by the five major payment brands-American Express, Discover, Japan Credit Bureau (JCB) International, MasterCard, and Visa
- Is a requirement of the industry NOT a law
- Failure to comply can result in hefty fines

PCI DSS

Build and Maintain a Secure Network

- Encrypt transmission of cardholder data across open and public networks
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Stored Cardholder Data

- Encrypt transmission of cardholder data across open and public networks

PCI DSS (Continued)

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- 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

PCI DSS (Continued)

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

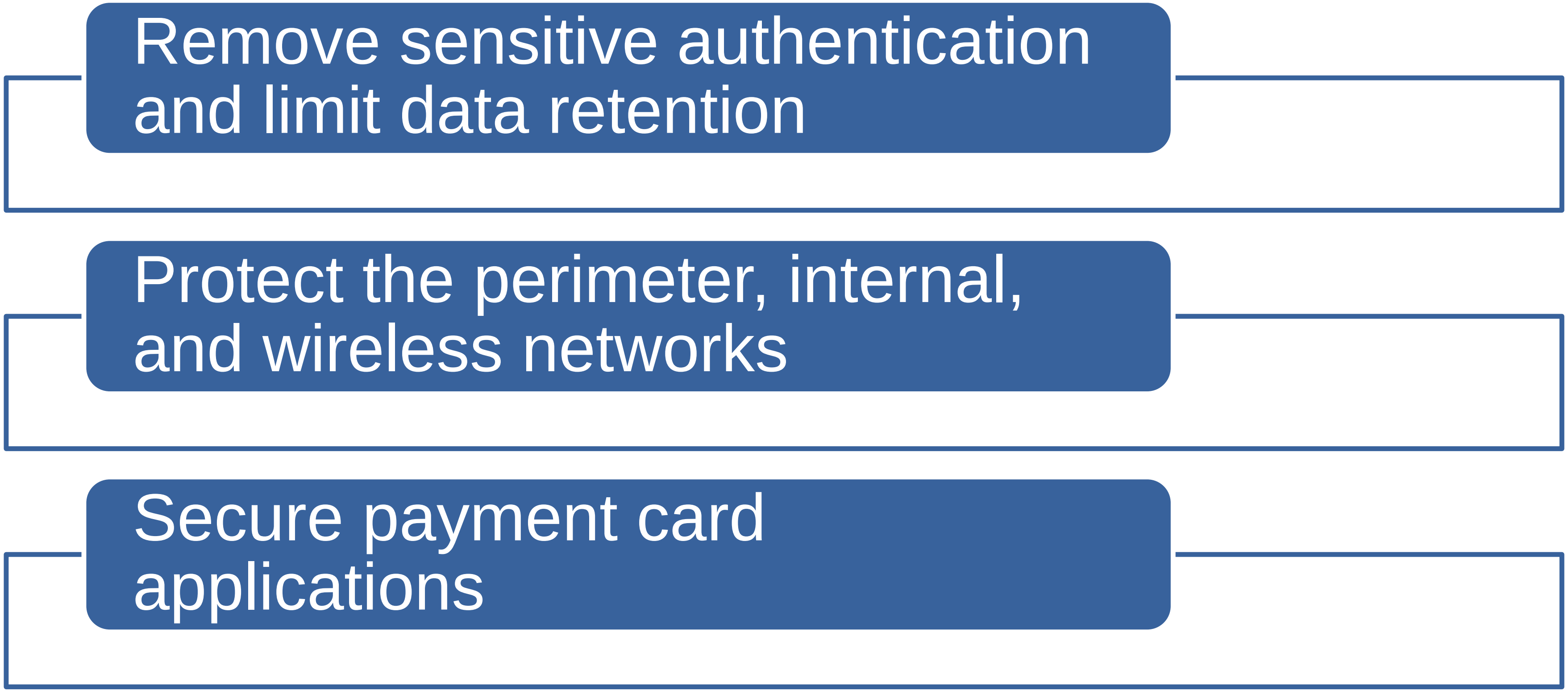
Maintain an Information Security Policy

- Maintain a policy that addresses information security

Impact for Noncompliance

- PCI DSS
  - Banks can be fined from $5,000 to $100,000 per month, which most likely passes the fine down to the offending business
  - Banks may terminate a noncompliant business merchant’s account
  - Banks may charge much higher transaction fees

PCI Compliance Framework Milestones



Remove sensitive authentication and limit data retention

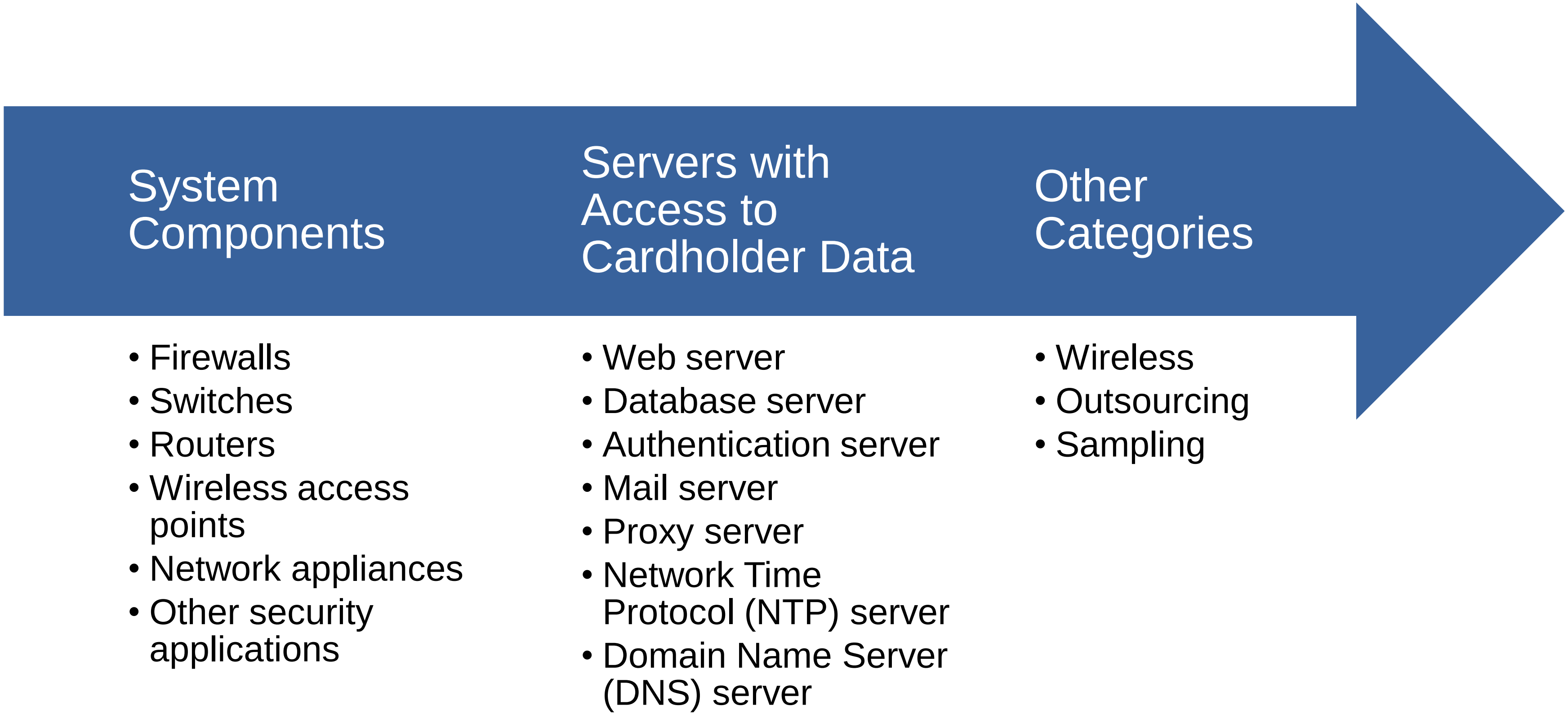
Protect the perimeter, internal, and wireless networks

Secure payment card applications

PCI Compliance Framework Milestones (Cont.)

- Monitor and control access to systems
- Protect stored cardholder data
- Finalize remaining compliance efforts and ensure all controls are in place

PCI Security Audits



System Components

- Firewalls
- Switches
- Routers
- Wireless access points
- Network appliances
- Other security applications

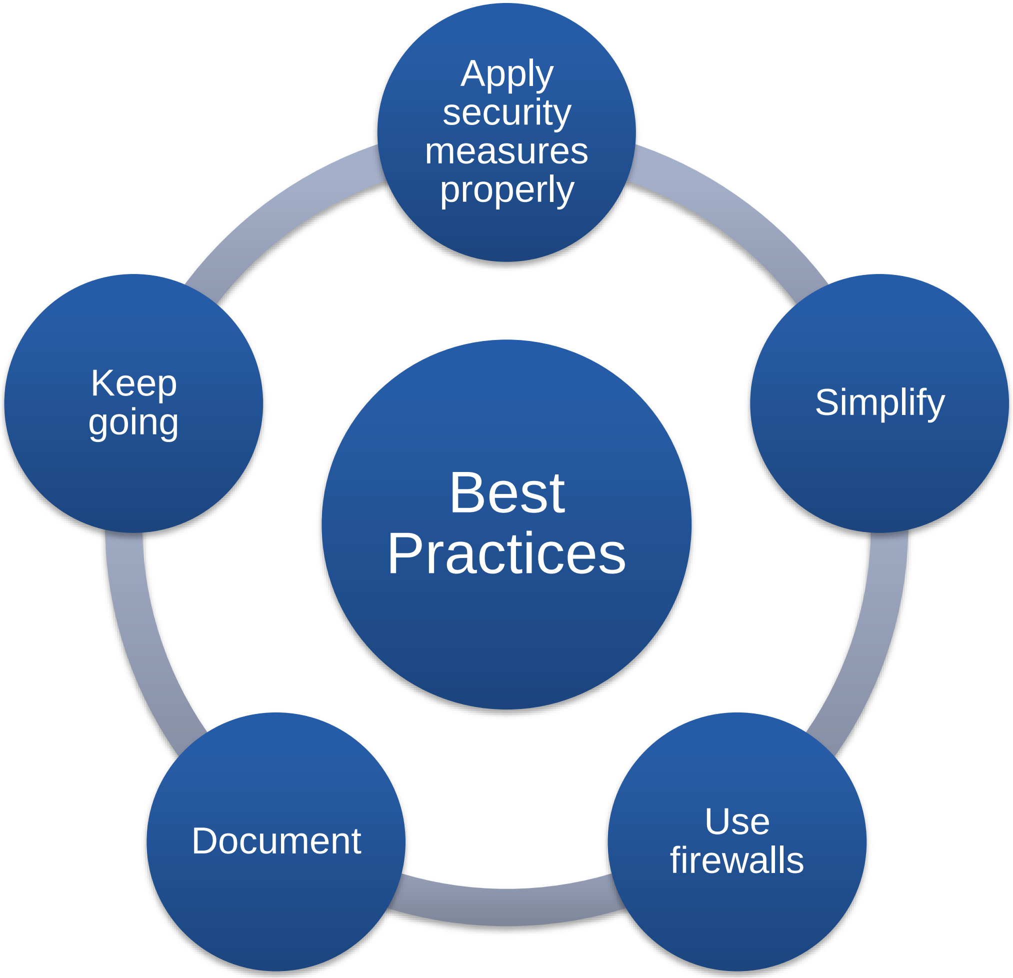
Servers with Access to Cardholder Data

- Web server
- Database server
- Authentication server
- Mail server
- Proxy server
- Network Time Protocol (NTP) server
- Domain Name Server (DNS) server

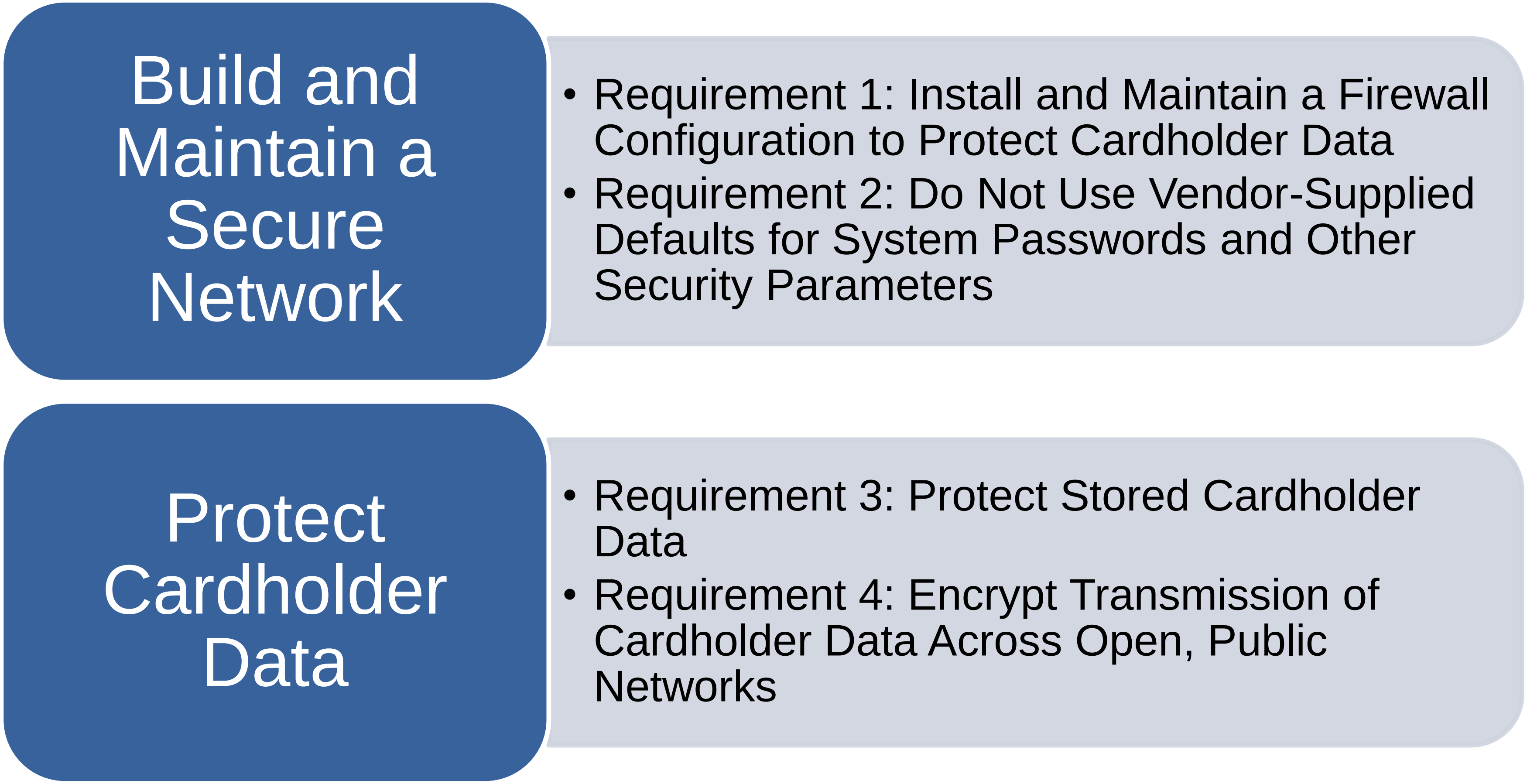
Other Categories

- Wireless
- Outsourcing
- Sampling

Best Practices to Mitioate Risk



PCI SSC Principles



Build and Maintain a Secure Network

- Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data
- Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Protect Cardholder Data

- Requirement 3: Protect Stored Cardholder Data
- Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

PCI SSC Principles (con't)

Maintain a Vulnerability Management Program

- Requirement 5: Use and Regularly Update Antivirus Software or Programs
- Requirement 6: Develop and Maintain Secure Systems and Applications

Implement Strong Access Control Measures

- Requirement 7: Restrict Access to Cardholder Data by Business Need-To-Know
- Requirement 8: Assign a Unique ID to Each Person with Computer Access
- Requirement 9: Restrict Physical Access to the Cardholder Data Environment

PCI SSC Principles (con’t)

Regularly Monitor and Test Networks

- Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data
- Requirement 11: Regularly Test Security Systems and Processes

Maintain an Information Security Policy

- Requirement 12: Maintain a Policy That Addresses Information Security for Employees and Contractors

Summary

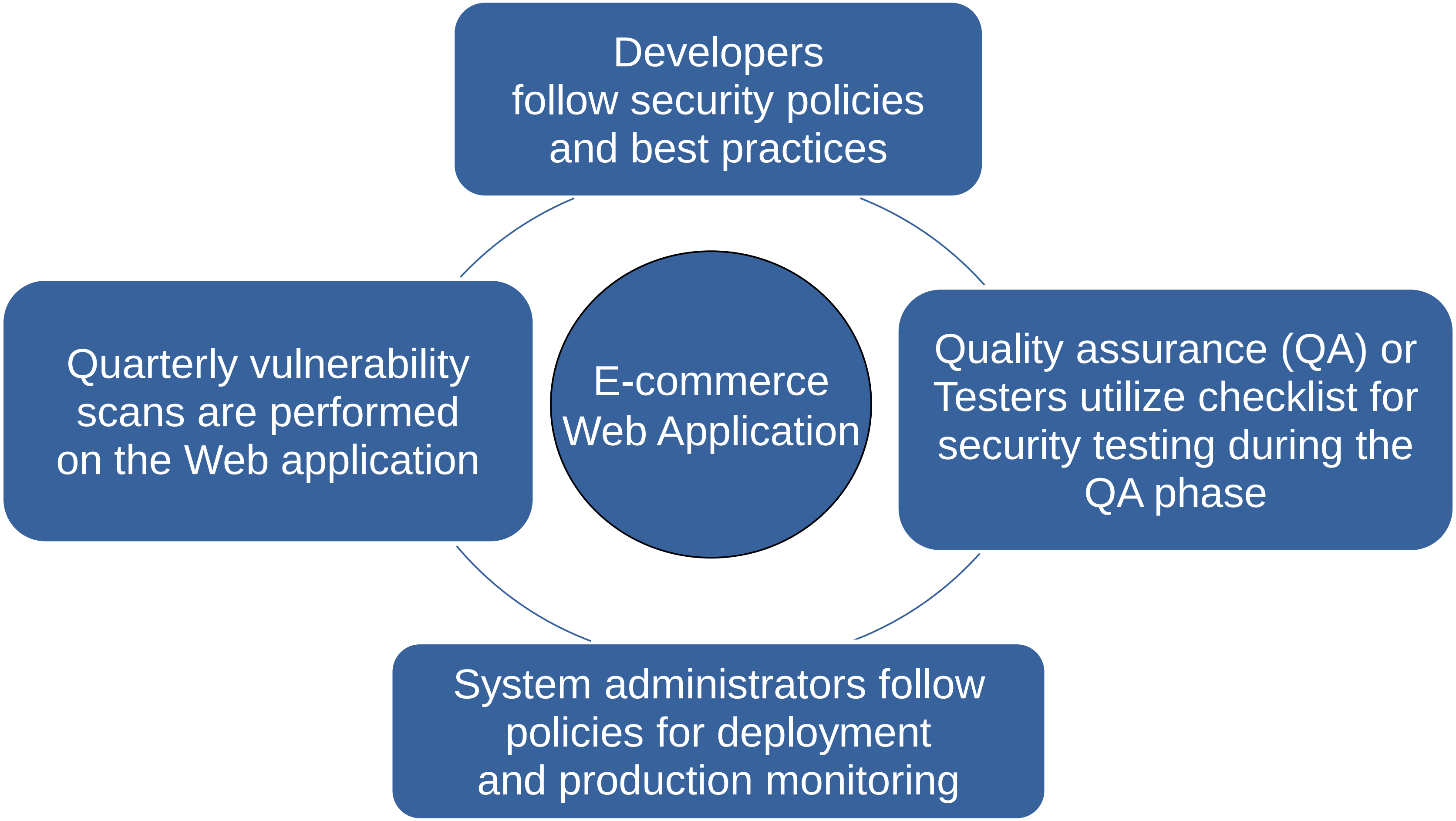
- Government regulations
- PCI DSS requirements
- Roadmap to compliance
- Who needs compliance
- Impact of noncompliance

Virtual Lab

- Applying Regulatory Compliance Standards

OPTIONAL SLIDES

PCI DSS Compliance Cycle for the Web Application



Developers follow security policies and best practices

Quality assurance (QA) or Testers utilize checklist for security testing during the QA phase

System administrators follow policies for deployment and production monitoring

Quarterly vulnerability scans are performed on the Web application

E-commerce Web Application