



Payment Card Industry Security Standards – PCI DSS, PCI-PTS and PA-DSS

**BASIS
SOFT EXPO 2012**

February 22-26, 2012



**Omar F. Khandaker, CISA, CISSP,
CISM, PMP
IT Consultant
Eastern Bank Limited
Board Member
ISACA Dhaka Chapter**

Source:
The PCI Security Standards Council
& The OWASP Foundation

Session Objective

Create Information Security awareness and take initiative to protect information asset of Bangladesh

AGENDA

- Security Challenges and Data Breach
- PCI Security Standards Council- PCI SSC
- Understand PCI DSS requirements
- Understand PA-DSS requirements
- **PCI DSS Compliance Challenges and Solutions**
- OWASP Top 10 and PCI DSS requirements
- Summary



Security Challenges & Data Breach

- Over 1B Records Breached from Database Servers in Past 6 years
- **\$214 per compromised record** and averaged \$7.2 million per data breach event
(Ponemon Institute, 2010 U.S. Cost of a Data Breach, October 2010)
- 48% Data Breaches Caused by Insiders
- 89% Records Stolen Using SQL Injection
- 86% Hacking Used Stolen Credentials

(Source: IDC, 2011, Verizon, 2007-2011)

Security Challenges & Data Breach..

2005 - The CardSystems

- **36 million Visa and MasterCard** Credit Card Data Stolen
- **Potential Financial Damage: Worldwide Total Unknown**
- **CardSystems** is an Arizona-based credit card processor faced reputational damage

2007 – TJ-Max

- **40 Million** Credit Data Stolen
- **Potential Financial Damage: US\$1 Billion**

Hackers gather data via wireless snooping

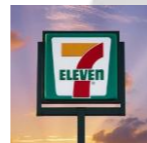
Security Challenges & Data Breach..

2008 – Best Western Hotel Chain

- Credit Card details of every guest stolen from chain's **1,312 hotels**
- **Potential Financial Damage: US\$4 billion**

This included guests' credit card numbers, addresses, and phone numbers, giving the thieves a perfect way to steal their identities.

2009 – The 7-Eleven



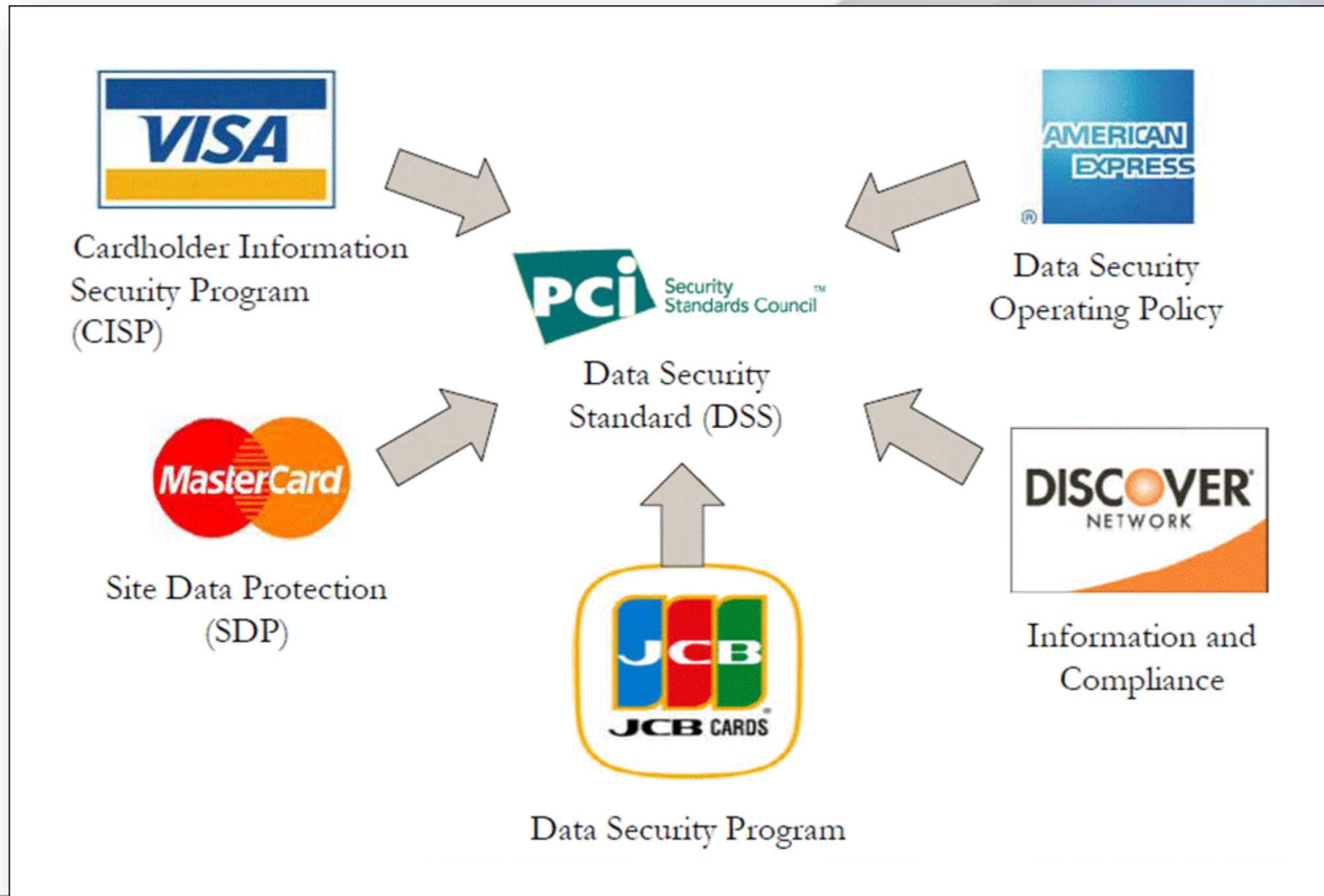
- **140 million** Credit Card Data Stolen
- **Potential Financial Damage:** Total damage unknown; **company has paid \$12 million** to card issuers
- Credit card processing company **Heartland Financial Systems** who processed credit card transactions for the 7-Eleven faced serious reputational issue. Hackers used “SQL injection attack” to steal the data.

Security Challenges & Data Breach..

2011- SONY PlayStation

- 100M personal data records stolen
- 12M Credit Card data stolen
- Potential Financial Damage: US\$3.8B
- 9% Drop in Share price

A unified Data Security Standard for Payment Card Industry



The PCI Security Standards Council (PCI SSC)

PCI SSC a global forum formally launched in 2006. They developed THREE sets of standards based on the industry segment:

PCI DSS – PCI Data Security Standard

Any entity of any size who accept payment cards, store, process, and/or transmit cardholder data is under PCI DSS compliance requirements.

PCI PTS – PCI PIN Transaction Security.

Device manufacturers like ATM, POS, etc. who handles Personal Identification Number (PIN) are under PCI-PTS requirements.

PA-DSS – Payment Application Data Security Standard.

Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements



The PCI SSC Security Ecosystem

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

PCI DSS – Payment Card Industry Data Security Standard

PCI Data Security Standard (PCI DSS),
which provides an actionable framework
for developing a robust payment card data
security process -- including prevention,
detection and appropriate reaction to
security incidents.



Who must comply?

Any entity of any size who accept payment cards, store, process, and/or transmit cardholder data is under PCI DSS compliance requirements.



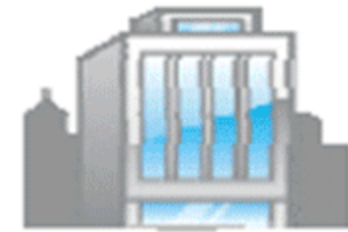
Merchants
(Accepting
Cards)



Acquirers
(Merchant Banks)



Issuers
(Cardholder
Banks)



Service
Providers
(Everybody Else)

PCI DSS Requirements

1. 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
2. Protect Cardholder Data	
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program	
Requirement 5	Use and regularly update anti-virus software or programs
Requirement 6	Develop and maintain secure systems and applications (6.5 - OWASP Guide, CWE/SANS Top 25, CERT Secure Coding)

PCI DSS Requirements

4. 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 cardholder data

5. 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

6. Maintain an Information Security Policy

Requirement 12	Maintain a policy that addresses information security
----------------	---

PCI DSS Compliance Challenges

- Assessment Planning
- Inappropriate Scoping
- Insufficient Documentation
- Application Vulnerability
- Unnecessary (or Inappropriate) Data Storage
- Compensating Controls

Key Challenge: **Assessment Planning**

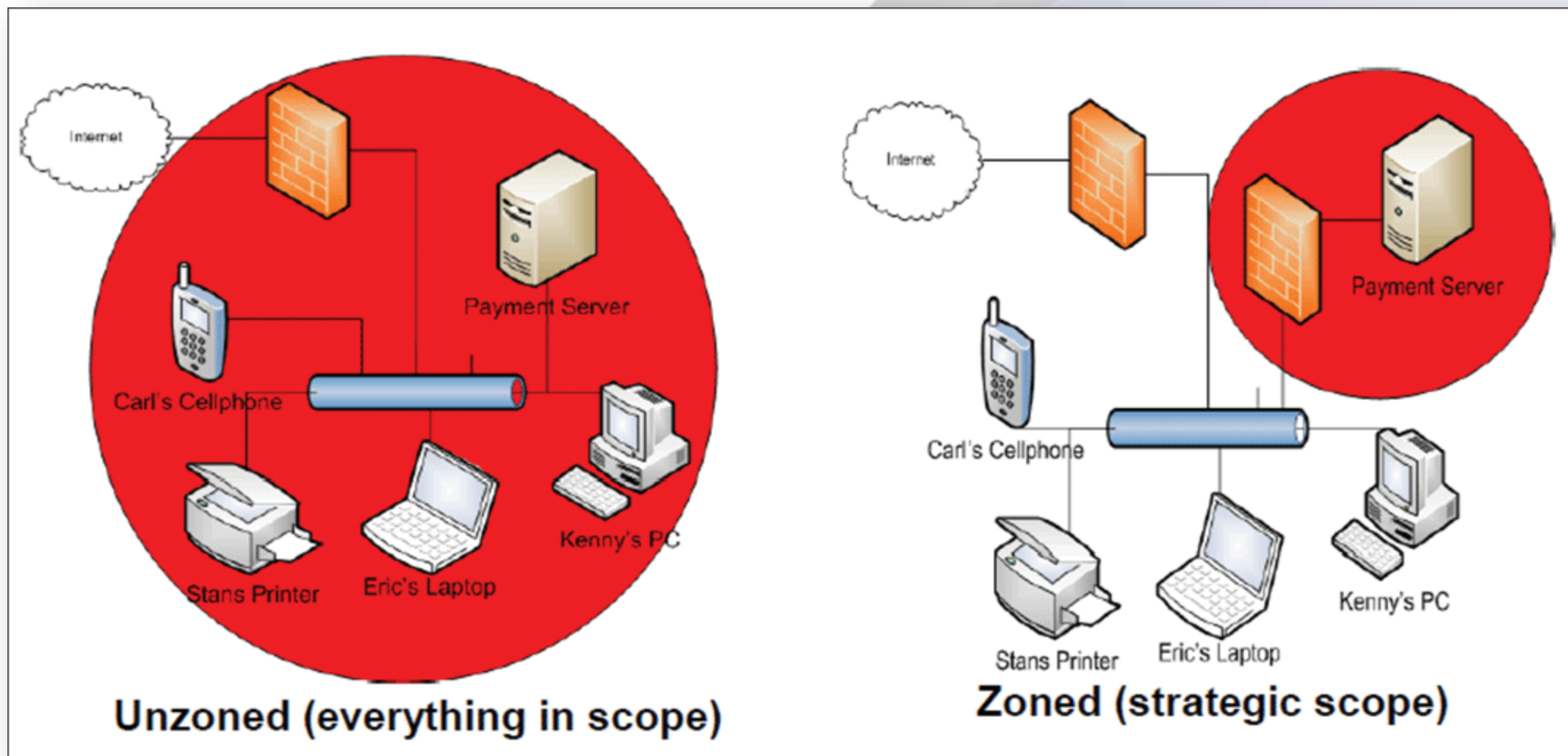
- **QSA (Qualified Security Assessors) validate the PCI DSS requirements in production environment**
- **Process, procedure, and guidelines should match with the production for proper onsite assessment**
- **QSA will go through onsite checklist published by PCI Security Standard Council**
- **Pre-assessment**
 - Do the pre-assessment questionnaire (even if you don't have to)
 - Go through a pre-assessment exercise and identify the gaps before start the onsite assessment

Key Challenge: Scoping

- PCI DSS applies to all system components i.e. network, server, or applications that are included or connected to the cardholder data environment.
- Cardholder Data Environment (CDE) is comprised of **people, processes and technology** that stores, processes, and/or transmits cardholder data or sensitive authentication data
- **Without proper scoping of the CDE, the entire organization comes under the scope of compliance for PCI DSS which increases Complexity & Cost**

Scoping Example

- Red area denotes scope of PCI assessment



Solution to Key Challenge **Scoping:** Enforcement of Scope

- **Once the scope of the CDE is defined that needs to be enforced with:**
 - ▶ Firewalls
 - ▶ Physical separation
- **Segmentation of CDE network from the Corporate network**
- **Satisfy QSA about CDE scoping through documentation:**
 - ▶ How zoning approach enforces the scope?
 - ▶ Why zoning approach is chosen?
 - ▶ Who is responsible for maintaining the boundary?

Key Challenge: Inadequate Documentation

■ Documentation is the key for compliance

- ▶ Organization must have documented policy, guidelines and procedures
- ▶ QSA (Qualified Security Assessor) must disregard ad-hoc or informal processes and documentation
- ▶ **Documentation is mandatory for each and every processes like patch update, anti-virus update, etc.**

Key Challenge: Application Vulnerability

- **Application Vulnerability control is critical to ensure the security of the CDE**
- **The requirements for application vulnerability assessment**
 - ▶ OWASP Guide (OWASP “Top Ten”), CWE/SANS Top 25, CERT Secure Coding
 - ▶ Lifecycle requirements
 - ▶ Requirements for code review and “application-level firewall” (this means “a web application firewall (WAF)”*)
- **Need to have a solid strategy for application security**

PCI DSS & OWASP Requirements

OWASP Guide, SANS CWE Top 25, CERT Secure Coding

6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:

Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

6.5.a Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.

6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.

6.5.c. Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:

PCI DSS & OWASP Requirements

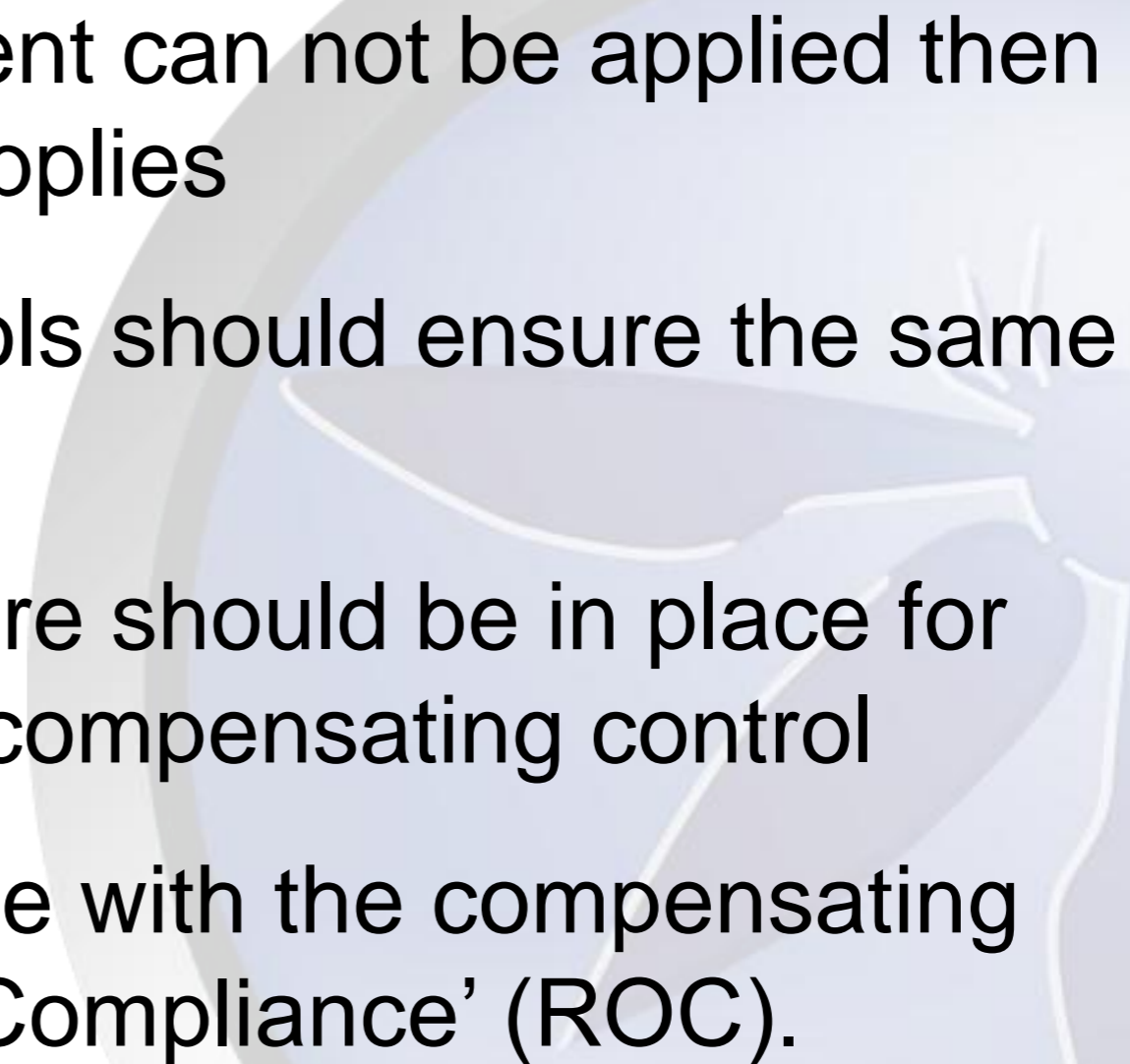
PCI DSS Requirements	Testing Procedures
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	6.5.1 Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)
6.5.2 Buffer overflow	6.5.2 Buffer overflow (Validate buffer boundaries and truncate input strings.)
6.5.3 Insecure cryptographic storage	6.5.3 Insecure cryptographic storage (Prevent cryptographic flaws)
6.5.4 Insecure communications	6.5.4 Insecure communications (Properly encrypt all authenticated and sensitive communications)
6.5.5 Improper error handling	6.5.5 Improper error handling (Do not leak information via error messages)
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). <i>Note: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.</i>	6.5.6 All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.
<i>Note: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):</i>	
6.5.7 Cross-site scripting (XSS)	6.5.7 Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	6.5.8 Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)
6.5.9 Cross-site request forgery (CSRF)	6.5.9 Cross-site request forgery (CSRF). (Do not rely on authorization credentials and tokens automatically submitted by browsers.)

Key Challenge: Data Storage

- **Transaction Authorization data can not be stored**
 - ▶ Never store full track data (magnetic-stripe) or CVV/CVC, PIN.
- There should be a good business reasons to store the PAN (full card number)
- Encrypting the PAN is the only approved way to store it
- Use **Triple-DES or AES** for PAN/Data encryption
- Consider a “secure data deletion” process to ensure security of cardholder data



Key Challenge: Inadequate Compensating Controls

- If particular requirement can not be applied then compensating control applies
 - Compensating Controls should ensure the same level of protection
 - Documented procedure should be in place for assessor to accept the compensating control
 - Assessor should agree with the compensating control for 'Report On Compliance' (ROC).
- 

PA-DSS

Formerly known as -PABP (Payment Application Best Practices) supervised by Visa

Goals

- ▶ Develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data
- ▶ Ensure their payment applications support compliance with the PCI DSS

The requirements for the PA-DSS are derived from the PCI DSS



PA-DSS Requirements



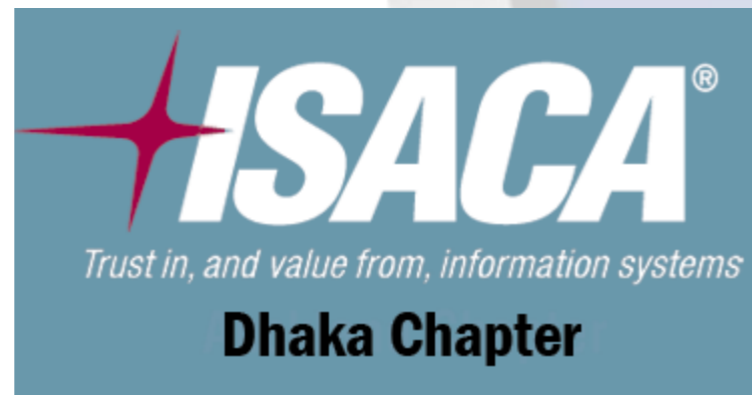
Requirement 1	Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data
Requirement 2	Protect stored cardholder data
Requirement 3	Provide secure authentication features
Requirement 4	Log payment application activity
Requirement 5	Develop secure payment applications (5.2 - OWASP Guide, SANS CWE Top 25, CERT Secure Coding)
Requirement 6	Protect wireless transmissions
Requirement 7	Test payment applications to address vulnerabilities
Requirement 8	Facilitate secure network implementation
Requirement 9	Cardholder data must never be stored on a server connected to the Internet
Requirement 10	Facilitate secure remote software updates
Requirement 11	Facilitate secure remote access to payment application
Requirement 12	Encrypt sensitive traffic over public networks
Requirement 13	Encrypt all non-console administrative access
Requirement 14	Maintain instructional documentation and training programs for customers, resellers, and integrators

Summary

- **Most issues are preventable, need awareness and initiatives**
- **Develop your own Data Security Standard (DSS) in line with international standards**
- **Launch Information Security Program**
- **To Achieve PCI Compliance:**
 - Proper Scoping and Planning is important
 - Identify the gaps through self-assessment
 - Separation of Duties, 'Need-to-know' and **Accountability** in place
 - Daily network monitoring and security logs
 - Update Security patches and anti-virus regularly
 - Quarterly vulnerability scanning of each system
 - Documented and **Tested** BCP, DR and Incident Response Plan
 - Comprehensive documentation for each processes and procedures

Thank You For Your Time!

Questions ?



References

- PCI SSC – www.pcisecuritystandards.org
- OWASP - www.owasp.org
- CERT - www.cert.org
- SANS - <http://www.sans.org>

