

# Intro to Payment Card Industry Data Security Standard (PCI DSS)

Tanya Baccam, CPA, CISSP, CISA, CISM, GCFW, GCIH,  
Oracle DBA, Senior SANS Instructor  
Baccam Consulting  
[tanya@securityaudits.org](mailto:tanya@securityaudits.org)



# Agenda

- Provide an overview of the PCI compliance process
- Identify key documents
- Review the individual PCI requirement areas
- Compensating controls

# Who's Affected by PCI?

- Anyone who processes, stores or transmits cardholder information
  - Focuses on the account number
  - Even if data is not stored, you may still be responsible
- Service Providers
  - “Service providers are organizations that process, store, or transmit Visa cardholder data on behalf of Visa members, merchants, or other service providers”
  - Generally, anyone who handles card account numbers but is not the merchant nor the Acquiring bank
- Merchants

# PCI DSS Key Roles

- PCI Service Provider
  - Any company that stores, processes, or transmits cardholder data on behalf of another entity.
- Approved Scanning Vendors
  - Authorized to perform the quarterly scans to show compliance with the PCI Data Security Standard.
- Qualified Security Assessors
  - Authorized to perform annual audits for merchants and service providers to document compliance with PCI

# Levels for Service Providers

Level	Definition	Compliance
Level 1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year	Annual Onsite PCI Data Security Assessment (QSA) and Quarterly Network Scans (ASV)
Level 2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	Annual PCI Self-Assessment Questionnaire and Quarterly Network Scans (ASV)

# Levels for Merchants

Level	Definition	Compliance
Level 1	<p>Any merchant processing more than 6,000,000 transactions per year</p> <p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise</p> <p>Any merchant identified by any card association as Level 1</p>	<ul style="list-style-type: none"> <li>* Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”)</li> <li>* Quarterly network scan by Approved Scan Vendor (“ASV”)</li> <li>* Attestation of Compliance Form</li> </ul>
Level 2	<p>Merchants processing 1 million to 6 million transactions annually</p>	<ul style="list-style-type: none"> <li>* Annual Self-Assessment Questionnaire (“SAQ”)</li> <li>* Quarterly network scan by ASV</li> <li>* Attestation of Compliance Form</li> </ul>
Level 3	<p>Merchants processing 20,000 to 1 million e-commerce transactions annually</p>	<ul style="list-style-type: none"> <li>* Annual SAQ</li> <li>* Quarterly network scan by ASV</li> <li>* Attestation of Compliance Form</li> </ul>
Level 4	<p>Merchants processing less than 20,000 e-commerce transactions annually and all other merchants processing up to 1 million transactions annually</p>	<ul style="list-style-type: none"> <li>* Annual SAQ recommended</li> <li>* Quarterly network scan by ASV if applicable</li> <li>* Compliance validation requirements set by acquirer</li> </ul>

# Self-Assessment Questionnaire

SAQ Validation Type	Description	SAQ: V1.2
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D



# Report on Compliance (ROC)

- Executive Summary
- Description of Scope of Work and Approach Taken
- Details about Reviewed Environment
- Contact Information and Report Date
- Quarterly Scan Results
- Findings and Observations



# Attestation of Compliance

- QSA Company Information
- Organization Information
- Type of Business
- Relationships
- Transaction Processing Information
- PCI DSS Validation
- Confirmation of Compliance Status
- QSA and Merchant/Provide Acknowledgements
- Action Plan for Non-compliant Status

# PCI Key Documents (1)

- PCI Data Security Standard
  - A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
  - [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)
- Payment Application Data Security Standard (PA-DSS)
  - Assists software vendors, etc. develop secure payment applications that do not store prohibited data, such as full magnetic stripe, other sensitive authentication data or PIN data, and ensure their payment applications support compliance with the PCI DSS.
  - PA-DSS requirements apply to payment applications that are sold, distributed or licensed to third parties.
- Supporting documents
  - [https://www.pcisecuritystandards.org/security\\_standards/supporting\\_documents.shtml](https://www.pcisecuritystandards.org/security_standards/supporting_documents.shtml)
  - [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_supporting\\_docs.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml)
- Prioritized Approach for DSS 1.2
  - <https://www.pcisecuritystandards.org/education/prioritized.shtml>

# PCI Key Documents (2)

- Navigating PCI DSS: Understanding the Intent of the Requirements
  - Designed for all merchants and service providers
- PCI DSS: Self-Assessment Guidelines and Instructions
  - Designed for all merchants and service providers
- PCI DSS: Self-Assessment Questionnaire A, B, C and Attestation
  - Designed for merchants. See the PCI DSS: Self-Assessment Guidelines and Instructions, "Selecting the SAQ and Attestation That Best Apply to Your Organization"
- PCI DSS: Self-Assessment Questionnaire D and Attestation
  - Designed for service providers and other merchants
- Fact Sheets
  - [https://www.pcisecuritystandards.org/education/fact\\_sheets.shtml](https://www.pcisecuritystandards.org/education/fact_sheets.shtml)
- PCI DSS 1.2 Changes Summary
  - [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_summary\\_of\\_changes\\_v1-2.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf)
  - Effective October 1, 2008

# Identifying In-scope Systems

- PCI DSS security requirements apply to all "system components"
  - A system component is defined as any network component, server or application that is included in or connected to the cardholder data environment
    - Network components = firewalls, switches, routers, wireless APs, network appliances, etc.
    - Servers = web, database, authentication, Domain Name Service (DNS), mail, proxy, Network Time Protocol (NTP), etc.
    - Applications = purchased and custom applications, including both internal and external (Web) applications
- The cardholder data environment is that portion of the network that possesses cardholder data or sensitive authentication data.
- Network segmentation can isolate the cardholder environment and can reduce the scope of the cardholder data environment.

# Third party providers

- Third party providers can manage components; however, the relevant third parties must be scrutinized either in
  - 1) each of the third party provider's clients' PCI audits
  - 2) the third party provider's own PCI audit.

# PCI DSS Example

**Build and Maintain a Secure Network**

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/Comments
<b>1.1</b> Establish firewall and router configuration standards that include the following:	<b>1.1</b> Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
<b>1.1.1</b> A formal process for approving and testing all network connections and changes to the firewall and router configurations	<b>1.1.1</b> Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
<b>1.1.2</b> Current network diagram with all connections to cardholder data, including any wireless networks	<b>1.1.2.a</b> Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	<b>1.1.2.b</b> Verify that the diagram is kept current.			

# PCI Requirement 1

- **Build and Maintain a Secure Network**
  - *Requirement 1: Install and maintain a firewall configuration to protect cardholder data*
    - 1.1 Establish firewall and router configuration standards
    - 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.
    - 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
    - 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 2

- **Build and Maintain a Secure Network**
  - ***Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters***
    - 2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
    - 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
    - 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access.
    - 2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 3

- **Protect Cardholder Data**
  - ***Requirement 3: Protect stored cardholder data***
    - 3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
    - 3.2 Do not store sensitive authentication data after authorization (even if encrypted).
    - 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).
    - 3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs)
    - 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse
    - 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 4

- **Protect Cardholder Data**
  - *Requirement 4: Encrypt transmission of cardholder data across open, public networks*
    - 4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.
    - 4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 5

- **Maintain a Vulnerability Management Program**
  - *Requirement 5: Use and regularly update anti-virus software or programs*
    - 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
    - 5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 6

- **Maintain a Vulnerability Management Program**
  - ***Requirement 6: Develop and maintain secure systems and applications***
    - 6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
    - 6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.
    - 6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle.
    - 6.4 Follow change control procedures for all changes to system components.
    - 6.5 Develop all web applications based on secure coding guidelines
    - 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 7

- **Implement Strong Access Control Measures**
  - *Requirement 7: Restrict access to cardholder data by business need to know*
    - 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
    - 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 8

- **Implement Strong Access Control Measures**
  - *Requirement 8: Assign a unique ID to each person with computer access.*
    - 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
    - 8.2 In addition to a unique ID, employ at least one of the following:
      - Password or passphrase
      - Two-factor authentication
    - 8.3 Implement two-factor authentication for remote access
    - 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography
    - 8.5 Ensure proper user authentication and password management for non-consumer users and administrators

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 9

- **Implement Strong Access Control Measures**
  - ***Requirement 9: Restrict physical access to cardholder data.***
    - 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
    - 9.2 Develop procedures to help all personnel easily distinguish between employees and visitors
    - 9.3 Make sure all visitors are properly handled
    - 9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three month.
    - 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.
    - 9.6 Physically secure all paper and electronic media that contain cardholder data.
    - 9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data
    - 9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area
    - 9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.
    - 9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 10

- **Regularly Monitor and Test Networks**
  - ***Requirement 10: Track and monitor all access to network resources and cardholder data.***
    - 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
    - 10.2 Implement automated audit trails for all system components
    - 10.3 Record at least the following audit trail entries for all system components for each event: user identification, type of event, data and time, success/failure identification, origination of event, identity or name of affected data, system components or resource
    - 10.4 Synchronize all critical system clocks and times.
    - 10.5 Secure audit trails so they cannot be altered.
    - 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 11

- **Regularly Monitor and Test Networks**
  - ***Requirement 11: Regularly test security systems and processes***
    - 11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.
    - 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change
    - 11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a subnetwork added to the environment, or a web server added to the environment).
    - 11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.
    - 11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# PCI Requirement 12

- **Maintain an Information Security Policy**
  - *Requirement 12: Maintain a policy that addresses information security for employees and contractors.*
    - 12.1 Establish, publish, maintain, and disseminate a security policy
    - 12.2 Develop daily operational security procedures that are consistent with requirements in this specification
    - 12.3 Develop usage policies for critical employee-facing technologies
    - 12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors
    - 12.5 Assign to an individual or team the security management responsibilities
    - 12.6 Implement a formal security awareness program
    - 12.7 Screen potential employees to minimize the risk of attacks from internal sources
    - 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers
    - 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2

# Hosting Provider Considerations

- Must adhere to the PCI DSS
- Special consideration should be given to:
  - A.1 Protect each entity's hosted environment and data,
    - A.1.1 Ensure that each entity only has access to own cardholder data environment
    - A.1.2 Restrict each entity's access and privileges to own cardholder data environment only
    - A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment
    - A.1.4 Enable processes to provide for timely forensic investigation
- Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not necessarily guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.

# Compensating Controls

- "Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk."
  - Must be documented by the assessor
  - Must be included in the ROC (Report on Compliance)
- A specific compensating control may not be sufficient in all environments – each environment needs to be evaluated after implementation to ensure effectiveness.
- Compensating controls must identify:
  - Constraints – Identify why the original requirement can not be met
  - Objective - Define the objective of the original control and the objective met by the compensating control
  - Identified risk - Identify any additional risk due to the lack of the original control
  - Definition of compensating controls - Define the compensating controls and explain how they address the objectives of the original control and increase risk, if any.

Reference: [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) - PCI-DSS v.1-2



# PCI DSS Compliance Steps

- Complete the Report on Compliance (ROC)
- Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV)
- Complete the Attestation of Compliance, for either Service Providers or Merchants
- Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

# Summary

- Obtained an overview of the PCI compliance process
- Reviewed key documents
- Reviewed the individual PCI requirements
- Examined Compensating controls



# Questions?

Thank you.