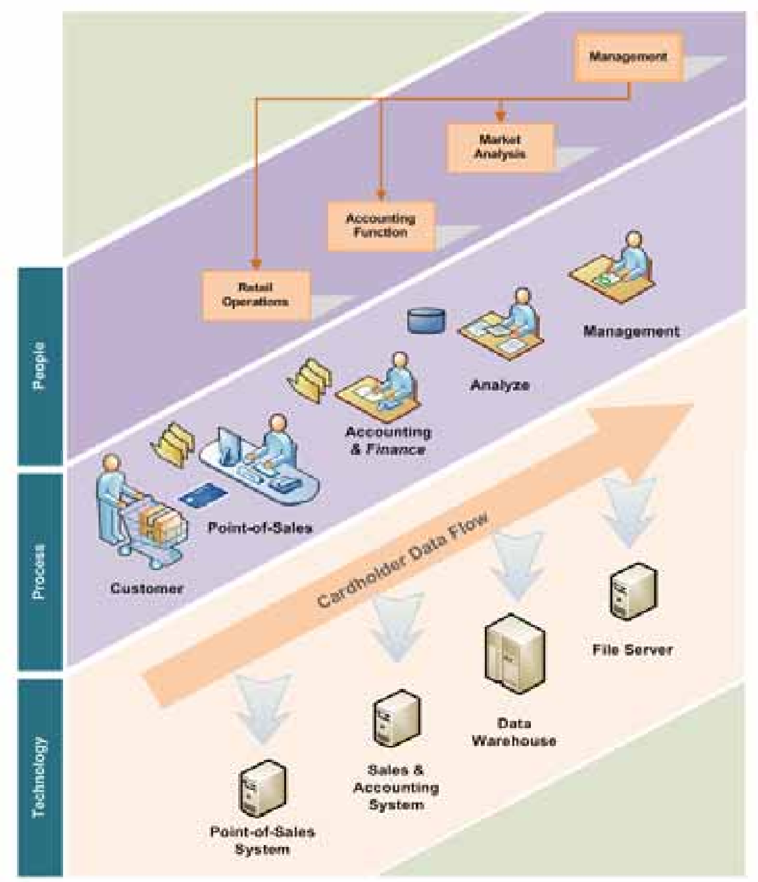
# PCI DSS Scope of Applicability

# Key Challenge – Scope of Compliance

- Applies to all entities that store, process or transmit cardholder data
- Applies to all system components defined as any network component, server, or application that is included in 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 and all requirements will apply.**

## Increased Complexity & Cost

# Key Challenges – Scope of Compliance

## Where is the data stored?

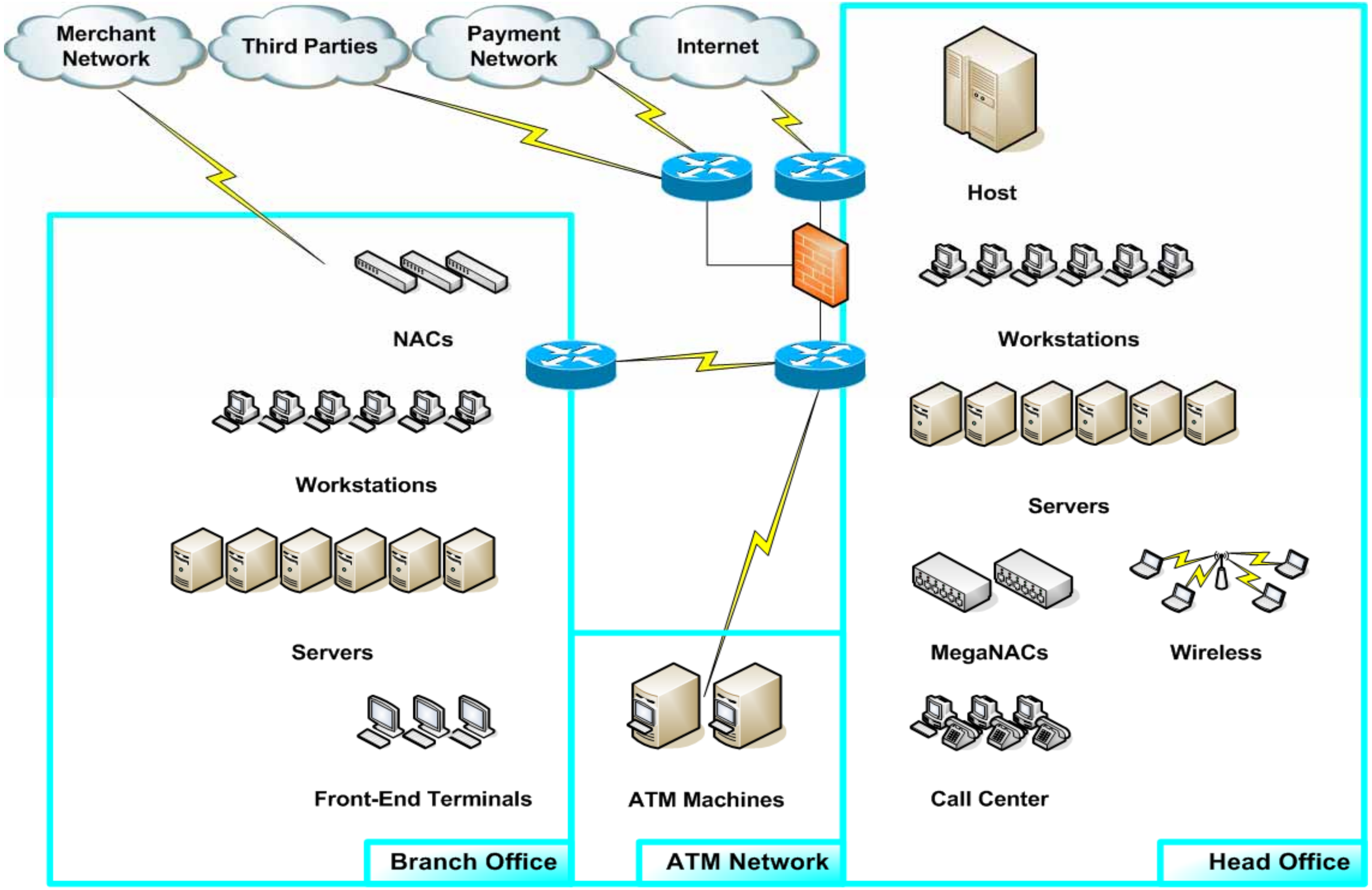
- Merchant Transactions
- ATM Electronic Journals
- Fraud Management Systems
- Call Center Voice and Screen Recordings
- Collections Management
- Statements and Billing Systems
- Local Databases, Spreadsheets and Reports

**Requirement 3.4 requires PAN to be rendered unreadable when stored.**

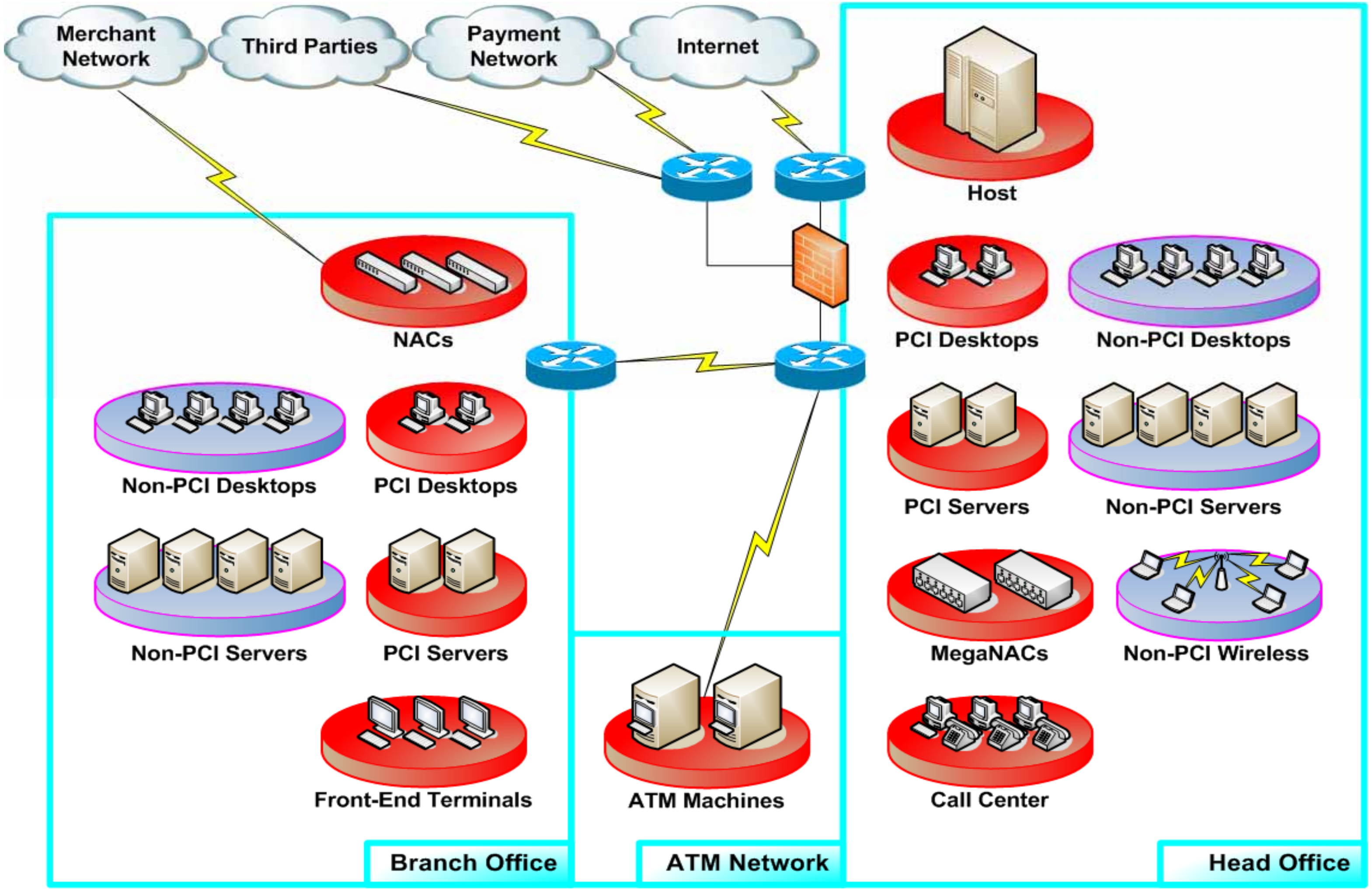
## Where is the data used?

- Merchant Acquiring Business (payment, settlement, reconciliation and reporting)
- Card Operations (account maintenance, card production, transaction monitoring and business analysis)
- Call Center (customer hotline and escalations)
- Authorization (manual authorizations)
- Finance and Accounting (dispute and reconciliation)
- Fraud Control (investigations)
- Card Collections (payment defaults)
- ATM Operations (transaction monitoring, cash replenishment

# Simplified Bank Network



# Identify In-Scope System Components



# Adequate Network Segmentation

## Per the PCI Data Security Standard (PCI DSS):

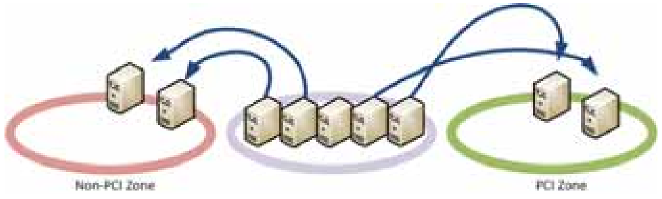
> *“Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method …”*
>
> *“Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network.”*

## Adequate Network Segmentation

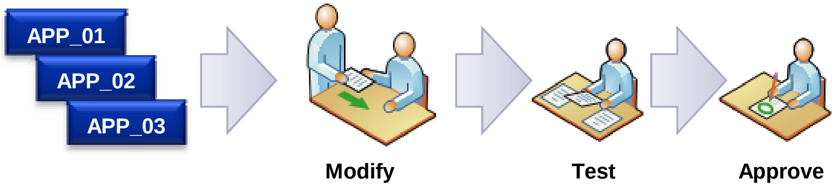
- Identify system components that store, process or transmit cardholder data.
- Segregate the in-scope system components into cardholder data environments (CDEs).
- Segment the CDE network using firewalls or routers with strong access control lists.

# Difficulty of Network Segmentation

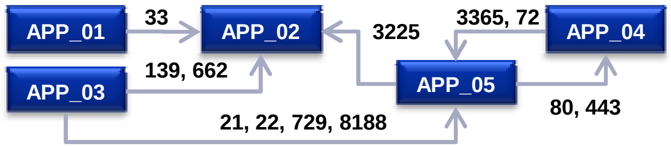
- Complex IP migration to create PCI zones
  - Possible business disruptions required for migration
  - Applications functionality may be impacted with IP address change



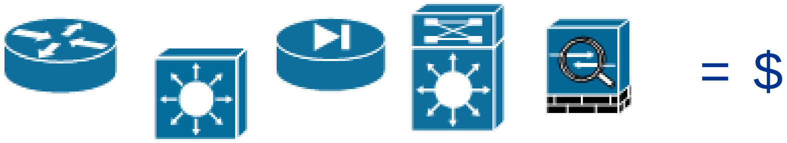
- Affected applications have to undergo testing
  - Increased demand on internal resources to test all affected applications
  - Cost incurred for modifying and testing outsourced applications



- Identifying and restricting all data flows – source IP, destination IP and network ports
  - Complex task to identify all communication flows between applications
  - Application functionality may be impacted with inaccurate identification of flow



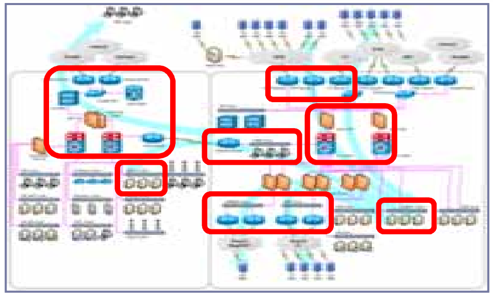
- Cost of acquiring and/or upgrading existing infrastructure
  - Procure more firewalls or routers
  - Upgrade of firewall or router hardware



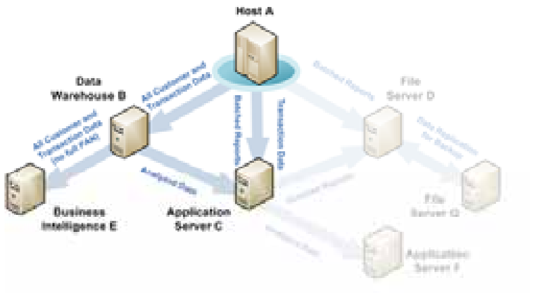
# Reduce Cardholder Data Footprint

## Determine feasibility of implementing scope reduction strategies on the cardholder data environment.

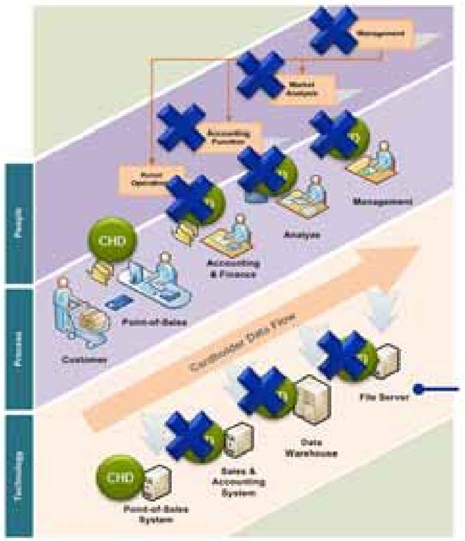
Network Segmentation of CDE System Components



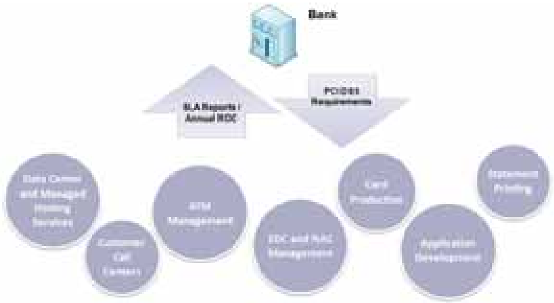
Reduce, Consolidate and De-Duplicate Data Storage



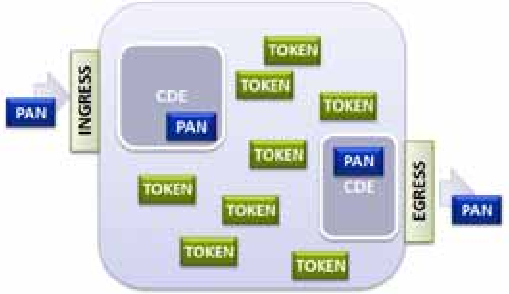
Eliminate Access and Use of Cardholder Data



Outsourcing of Payment-Related Functions



Tokenization Solutions



# Deep Dive of PCI DSS Requirements

# Analysis by Categories

**PCI DSS requirements can be further classified into seven categories.**

1. **Data Controls**
   - Information Classification and Handling
   - Information Access
   - Data Encryption
   - Data Flow
2. **Network Controls**
   - Architecture
   - Firewall
   - Intrusion Detection/Prevention
3. **System Controls**
   - Hardening
   - Patching
   - Integrity
4. **Application Controls**
   - Software Development Lifecycle
   - Application Firewall
   - Source Code Reviews
5. **Auditing/Logging Controls**
   - Log Management
   - Log Analysis
6. **Policy Controls**
   - PCI DSS requirements
7. **Physical Controls**
   - Access and monitoring

# Data Controls

- Understand the data flow to ensure adequate information classification and handling.
- Control information access and implement data protection.

# Data Controls

**3.1**

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.

**4.2**

Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

**Keep storage to a minimum.**

## Don’t Need It? Don’t Store It!

- Assess and reengineer your business processes to eliminate or consolidate the use of cardholder data.
- Perform data de-duplication to reduce storage in systems.
- Cardholder data retention must be limited only to that required for business, legal, and/or regulatory purposes.
- Require quarterly automatic or manual process to identify and securely delete cardholder data.

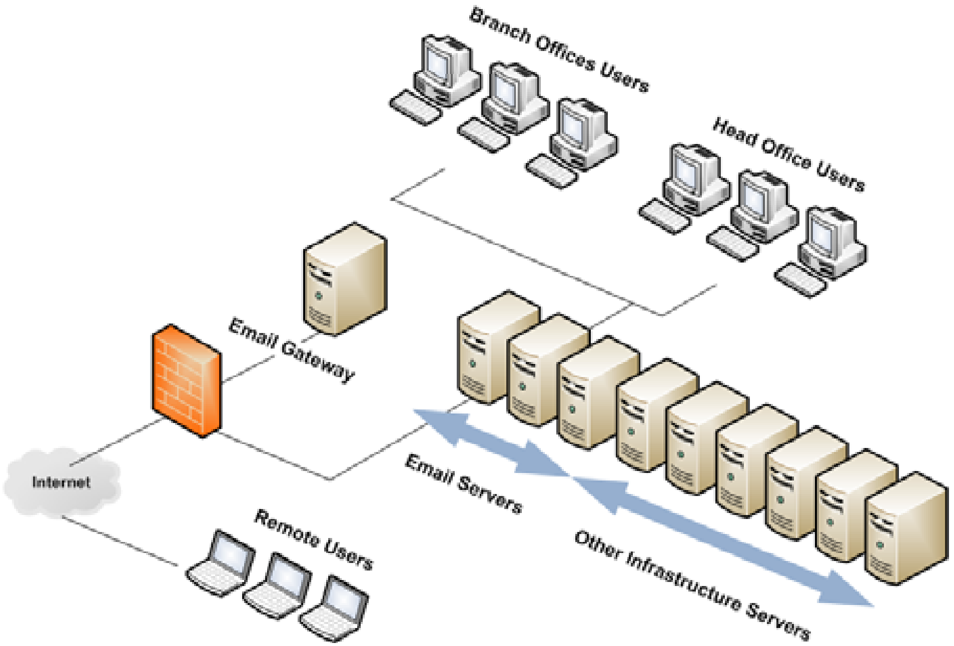
## Use of End User Messaging

- End-user messaging technologies should not be used if possible.
- Must be managed to reduce the risk of data leakage.

# Avoid End-User Messaging Technologies

**For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.**

- Unprotected PAN should not be sent using end-user messaging technologies.
- Even with protected PAN, use of such technologies increases the complexity and cost of compliance as the messaging infrastructure will be in compliance scope.
- Difficult to segment messaging infrastructure from rest of the technology environment.



# Data Controls

**3.2**

Do not store sensitive authentication data after authorization (even if encrypted).

**3.2.1**

Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

**3.2.2**

Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

## Storage of Sensitive Authentication Data

- NEVER store sensitive authentication data SUBSEQUENT to authorization.
- NEVER a good reason to store sensitive authentication data.
- NEVER store FULL track data but may retain data elements needed for business (e.g. PAN, expiry date and service code).
- If sensitive authentication data is received and deleted, QSA to obtain and review the processes for deleting the data to verify that the data is unrecoverable.
- Storage permitted for issuing parties but require legitimate documented business justifications.

**Do not store in any situation.**

# Data Controls

**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, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography (hash must be of the entire PAN), Truncation (hashing cannot be used to replace the truncated segment of PAN), Index tokens and pads (pads must be securely stored), and Strong cryptography with associated key-management processes and procedures.

## Secure the Pan

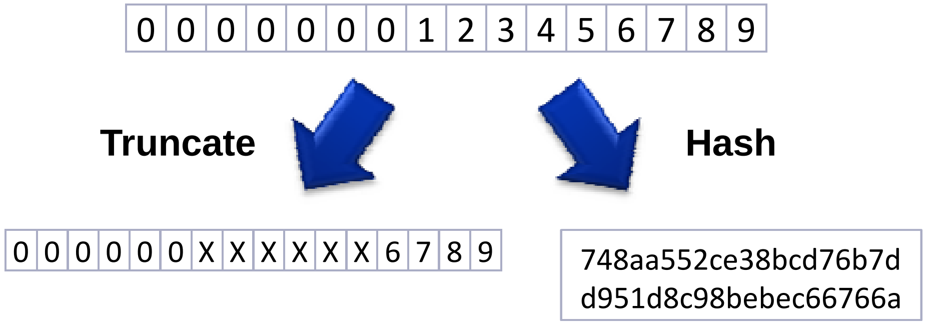
- Masking does not apply to employees and other parties with a legitimate business need to see the full PAN.
- Be mindful of personnel with access to lists of full PAN and ability to offload data (e.g. Internet access, external mail, portable media, etc).
- Does not supersede stricter payment brand requirements in place for displays of cardholder data (e.g. only last 4 digits for point-of-sale receipts).
- PAN must be rendered unreadable when stored including media (e.g. voice recordings, paper, etc).
- Avoid storing both truncated and hashed PANs.

**Never store PAN in the clear.**

# Avoid Storing Both Truncated and Hashed PANs

**It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity‘s environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. (Requirement 3.4)**

- Storing both truncated and hashed PANs weakens the security strength of the hashed PAN.
- Additional controls needed to prevent correlation of truncated and hashed PANs.
- Avoid such implementations if possible to reduce complexity of compliance.



| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Truncate

Hash

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | X | X | X | X | X | X | 6 | 7 | 8 | 9 |

748aa552ce38bcd76b7d
d951d8c98bebec66766a

*Without truncated PAN =* $10^{16}$
*With truncated PAN =* $10^{6}$ *= 1M numbers*

**Computationally Feasible!**

# Data Controls

**7.1.2**

Assignment of privileges is based on individual personnel’s job classification and function.

**7.1.3**

Requirement for a documented approval by authorized parties specifying required privileges.

**8.5.2**

Verify user identity before performing password resets.

**8.5.8**

Do not use group, shared, or generic accounts and passwords, or other authentication methods.

## Role-Based Access Control

- Privileges should be assigned to individuals based on job classification and function (also called “role-based access control” or RBAC).
- Authorization form is required for all access, including IT personnel and business users.
- Authorization form must specify required privileges at a reasonably granular level, and signed off by management.
- Password reset requests using non-face-to-face methods must require verification of user identity.
- Shared accounts should be prohibited.
- Take note of how default administrator, service and application accounts or managed.

# Network Controls

- Implement secure network architecture
- Ensure adequate protection using firewalls and intrusion detection/prevention systems

# Network Controls

**8.3**

Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

**8.5.6**

Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.

## Remote Network Access Control

- Remote access to system components in scope will require two-factor authentication.
- Includes employees, administrators and third parties.
- Vendor access for remote maintenance must be controlled and activated only for the period required.
- Vendor access must be monitored.

# Network Controls

**12.3.8**

Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.

**12.3.9**

Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

**12.3.10**

For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

## Remote Network Access Control

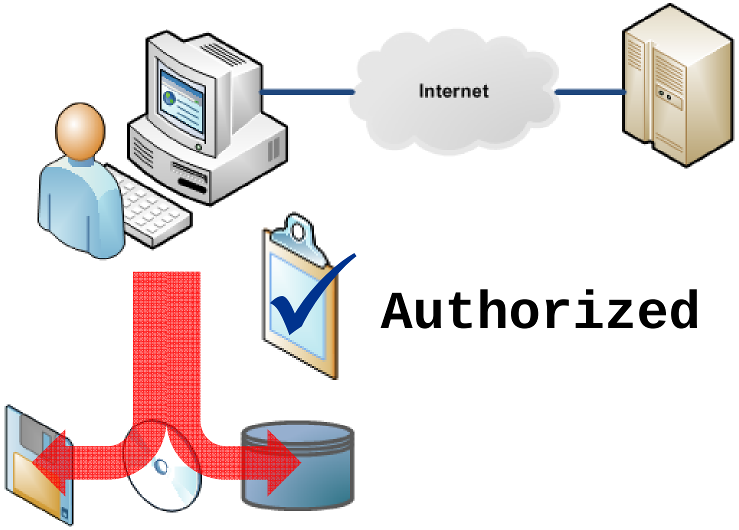
- Automatic disconnect of remote access sessions required. *(Note: Inactivity period not specified.)*
- Vendor and business partner remote access must be controlled and activated only when required.
- Data extraction onto local hard drives and removable electronic media should be avoided and if allowed, must be explicitly authorized for a defined business need.

# Increased Flexibility for Personnel on Remote Access

**For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, <u>unless explicitly authorized for a defined business need</u>. (Requirement 12.3.10)**

**For personnel with proper authorization, verify that <u>usage policies require the protection of cardholder data</u> in accordance with PCI DSS Requirements. (Requirement 12.3.10.b)**

- Flexibility to allow explicitly authorized personnel access.
- Data accessed remotely must be protected in accordance with the standard.
- Authorization with defined business need must be documented.



# Network Controls

**1.1**

Establish firewall and router configuration standards that include the following:

**1.1.2**

Current network diagram with all connections to cardholder data, including any wireless networks.

**1.1.4**

Description of groups, roles, and responsibilities for logical management of network components.

## Firewall and Router Standards

- Document cardholder data flow in the network diagram.
- Document a description of groups, roles and responsibilities for logical management of network components.

# Network Controls

**1.1.5**

Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

**1.1.6**

Requirement to review firewall and router rule sets at least every six months.

## Firewall and Router Standards

- Document the list of services and ports necessary for business.
- Provide justification and documentation for any available protocols besides HTTP, SSL, SSH and VPN.
- Firewall and router rule sets must be reviewed at least every 6 months with documented report.
- Note linkages between change management, justification documentation and rule set reviews.

# Network Controls

**1.3**

Prohibit direct public access between the Internet and any system component in the cardholder data environment.

**1.3.6**

Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)

**1.3.7**

Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

## Firewalls and Zones

- Firewalls must implement stateful packet inspection – Routers with Access Control Lists (ACLs) are NOT firewalls.
- Non-traditional firewalls allowed but must still implement stateful inspection.
- All databases (data repositories) must be implemented in the internal network.
- Any cardholder data present in DMZ = Non-compliance.
- Watch out for FTP servers in the DMZ that end up as data repositories.

# Network Controls

1.2.3

Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

## Firewalls and Zones

- Firewall between wireless networks and payment card environment (NOTE: Wireless NOT only 802.x).
- Must be implemented even if cardholder data does not flow over the wireless network.

# Network Controls

4.1

Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: The Internet, Wireless technologies,Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).

4.1.1

Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

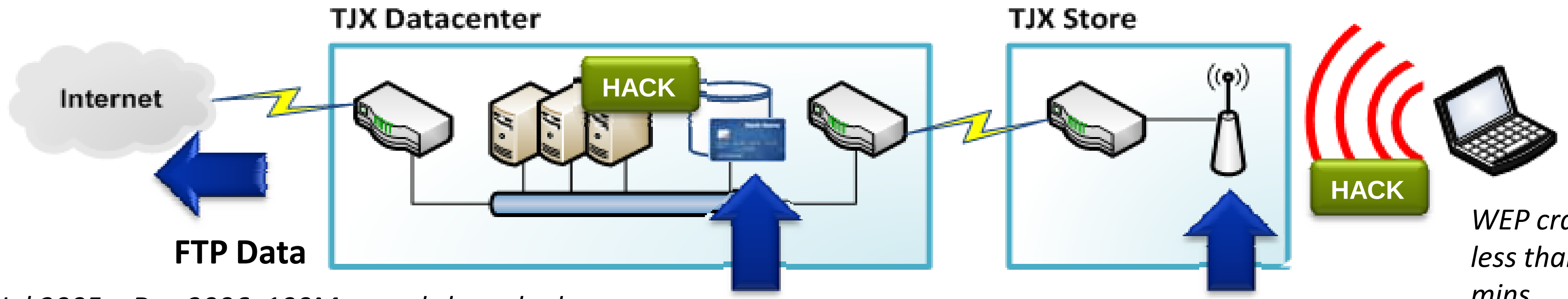
## Encrypt Data Over Open, Public Networks

- Open networks – Internet, WIFI, GSM, GPRS, Satellite.
- Internal networks do not require encrypted transmission.
- Check Payment Brand rules specific to the use of cellular technologies.
- Wireless is a risk area with cases of real world data breaches and watch out for use of wireless POS terminals.
- For new wireless implementations, WEP is prohibited. For current wireless implementations, use of WEP prohibited after June 30, 2010.
- Note requirement for use of industry best practices for wireless implementations (e.g. TKIP vs. AES).

# Avoid Wireless in Cardholder Data Environment

**Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.**

- Wireless is still considered a risk with real world data breach cases.
- WEP first broken in 2001 and can now be cracked in seconds.
- Some WPA and WPA2 implementations and scenarios can be broken in minutes



- *From Jul 2005 – Dec 2006, 100M records breached.*
- *Settled with MasterCard for US$24M and Visa for US$40.9M, etc*

**Track 2 Data Stored in Violation**

**WEP with SSID Broadcast**

*WEP cracked in less than 30 mins*