Course Overview and Objectives

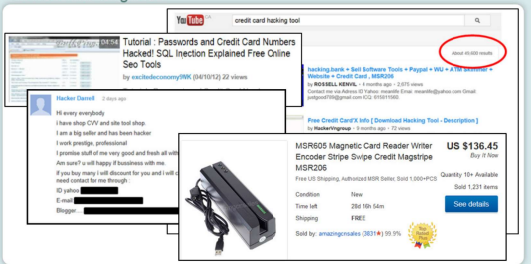
Course Overview

- Why We Are Here
- PCI Overview
- Compliance Programs and PCI Program Role
- Assessor Responsibilities and Program Requirements
- Cardholder Data Discovery and Scoping
- PCI DSS v3.2 Requirements
- Information Supplement and Reporting Overview
- Final Exam

Course Objectives:

- Provide a fundamental understanding of the Payment Card Industry
- Discuss the different organizations within the Payment Card Industry
- Prepare candidates for the next level of PCI DSS training
- Provide payment industry definitions, relationships, industry-specific technology, and payment flow processes
- Discuss cardholder data discovery
- Discuss options for reducing the scope of a PCI DSS assessment
- Understand intent of the PCI DSS Requirements
- Locate and use the various PCI SSC Information Supplements
- Discuss ROC documentation
- Describe appropriate uses of compensating controls

How is Data Targeted?



Payment Card Data is a Target

According to industry reports*:

- 2012 – Payment card data made up 48% of data breaches investigated and was also the 2nd largest volume of records affected
- 2013 – Payment card data targeted in 61% of breaches investigated

The following methods were identified as being used to remove stolen data from the environments*:

- 76% exploited weak or stolen credentials
- 52% involved some form of hacking
- 40% incorporated malware
- 35% involved physical attacks
- 29% leveraged social tactics

* Sources: Trustwave 2013 Global Security Report & Verizon Data Breach Investigations Report 2012 and 2013

How is Data Targeted? (Contd.)

Skimming

Copying payment card numbers either by tampering with:

- POS Devices
- ATMs
- Kiosks

Or by copying the card's magnetic stripe manually using handheld skimmers.

Spot the Difference?

(click image to reveal)

Handheld skimmers are small enough to be concealed easily and can capture data from thousands of cards.

How is Data Targeted? (Contd.)

Phishing

Reconraissance
- Information gathering from various online sources and social networking sites
- Business applications and software

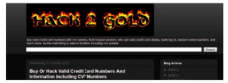
Social Engineering
- Phishing emails or messages coming from a target's social network
- Phone call from assumed known entity

Break-In
- Delivery through email
- Software vulnerabilities

How is Payment Data Monetized?

Common methods for monetizing stolen card data:

- Skimmed full track data and transaction information used to replicate a physical payment card, which can then be used for fraudulent transactions in face-to-face environments, or ATM transactions
- Captured cardholder data is used where card-not-present transactons are accepted, such as e-commerce or mail-order / telephone order (MO/TO) transactions
- Stolen cardholder data and sensitive authentication data are sold in bulk to other criminals who perform their own fraud using the stolen data



How Is Payment Data Monetized? (Contd.)

Police bust credit card hackers who stole 160 million cards

According to the indictment, US credit card numbers sold for about $10 each, Canadian numbers cost $15 and European ones - most of which are protected with more secure chip-and-pin technology - for $50.

Who is Targeted?

Commonly targeted industries* include:
- Retail – 45% of breaches
- Food and Beverage – 24% of breaches
- Hospitality – 9% of breaches
- Financial Services – 7% of breaches
- Nonprofit – 3%

Franchise Point-of-Sale (POS) Systems Targeted
Hackers target small businesses
Major Corporations Attacked
Hackers Target Credit Card Processing Companies
Subscription software vendors lucrative targets
Hotels: hackers' favourite target
Restaurant POS Systems a Major Target For Hackers
Cloud Services Get Hacked
Retailers Targeted

* Sources: Trustwave 2013 Global Security Report & Verizon Data Breach Investigations Report 2012 and 2013

Who is Targeted? (Contd.)

Major payment card processor (2005) – 40 million cards lost
- Accessed a database with direct connectivity to the Internet
- Company no longer in business

Payment processor (2009) – 160 million cards lost
- Malware was used to capture cardholder data as it was processed
- Reports suggest direct costs for the breach cost 171 million USD

US food based retailer (2013) – 1.8 million cards lost
- Malware installed at the POS was skimming account data as data was captured
- Estimated costs could exceed 80 million USD

Major retailer (2013) – over 100 million cards lost
- Malware installed on point-of-sale systems to capture cardholder data in memory
- Senior staff members resigned following breach

Major retailer (2014) – over 50 million cards lost
- Malware installed on point-of-sale systems to capture cardholder data in memory

Module Overview and Objectives

Module Topics:

- PCI SSC and Standards Overview
- Payment Industry Terminology
- Payment Transaction Flow
- Service Provider Relationship

Module Objectives:

After completing this module, you will be able to:
- Describe the role of the Payment Card Industry Security Standards Council
- Outline the Payment Card Industry Security Standards
- Describe the lifecycle followed for changes to standards
- Define Payment Card Industry terminology
- Define the processes involved in card processing: Authorization, Clearing, and Settlement
- Define service provider relationships

Knowledge Check

Methods for stealing payment card data include:

a) Malware

b) Weak passwords

c) Physical skimming

d) All of the options are correct

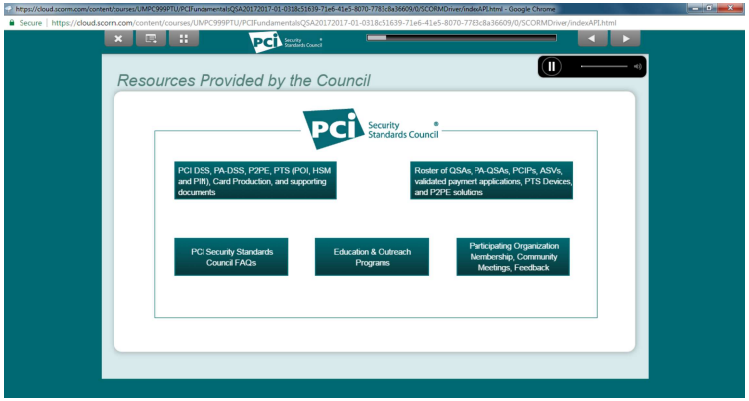
Next

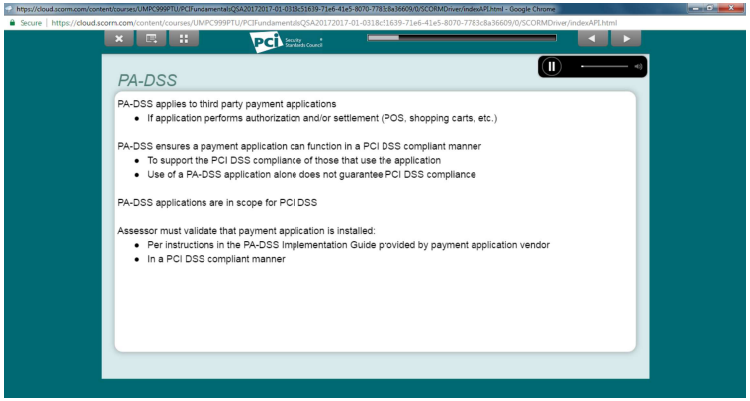
What is the PCI SSC?

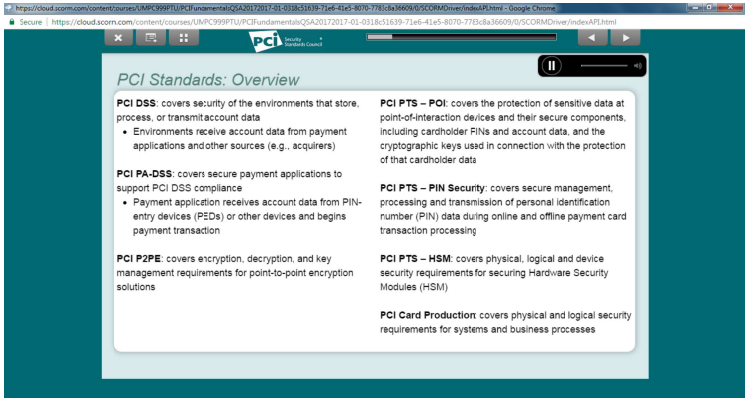
The PCI SSC is an independent industry standards body providing oversight of the development and management of Payment Card Industry Data Security Standards on a global basis.

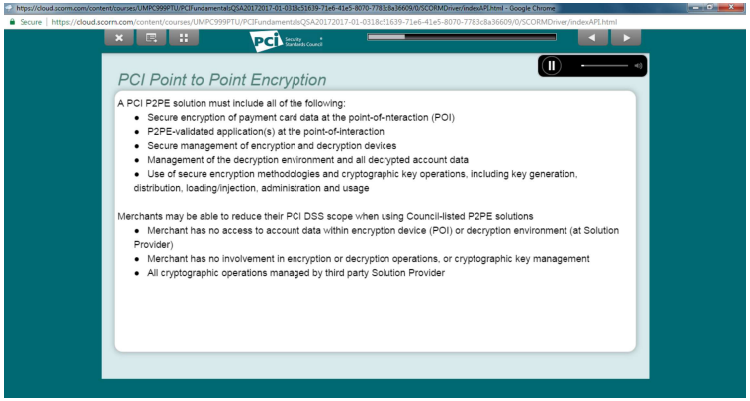
The PCI SSC provides training for several different qualifications and programs.

PCI SSC founding payment brands include:
- American Express
- Discover Financial
- JCB International
- MasterCard
- Visa, Inc.


Resources Provided by the Council
PCI Security Standards Council
PCI DSS, PA-DSS, P2PE, PTS (POI, HSM and PIN), Card Production, and supporting documents
Roster of QSAs, PA-QSAs, PCIPs, ASVs, validated payment applications, PTS Devices, and P2PE solutions
PCI Security Standards Council FAQs
Education & Outreach Programs
Participating Organization Membership, Community Meetings, Feedback


PA-DSS
PA-DSS applies to third party payment applications
If application performs authorization and/or settlement (POS, shopping carts, etc.)
PA-DSS ensures a payment application can function in a PCI DSS compliant manner
To support the PCI DSS compliance of those that use the application
Use of a PA-DSS application alone does not guarantee PCI DSS compliance
PA-DSS applications are in scope for PCI DSS
Assessor must validate that payment application is installed:
Per instructions in the PA-DSS Implementation Guide provided by payment application vendor
In a PCI DSS compliant manner


PCI Standards: Overview
PCI DSS: covers security of the environments that store, process, or transmit account data
Environments receive account data from payment applications and other sources (e.g., acquirers)
PCI PA-DSS: covers secure payment applications to support PCI DSS compliance
Payment application receives account data from PIN-entry devices (PEDs) or other devices and begins payment transaction
PCI P2PE: covers encryption, decryption, and key management requirements for point-to-point encryption solutions
PCI PTS – POI: covers the protection of sensitive data at point-of-interaction devices and their secure components, including cardholder PINs and account data, and the cryptographic keys used in connection with the protection of that cardholder data
PCI PTS – PIN Security: covers secure management, processing and transmission of personal identification number (PIN) data during online and offline payment card transaction processing
PCI PTS – HSM: covers physical, logical and device security requirements for securing Hardware Security Modules (HSM)
PCI Card Production: covers physical and logical security requirements for systems and business processes


PCI Point to Point Encryption
A PCI P2PE solution must include all of the following:
Secure encryption of payment card data at the point-of-interaction (POI)
P2PE-validated application(s) at the point-of-interaction
Secure management of encryption and decryption devices
Management of the decryption environment and all decypted account data
Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage
Merchants may be able to reduce their PCI DSS scope when using Council-listed P2PE solutions
Merchant has no access to account data within encryption device (POI) or decryption environment (at Solution Provider)
Merchant has no involvement in encryption or decryption operations, or cryptographic key management
All cryptographic operations managed by third party Solution Provider

PCI DSS: Relationship to PA-DSS and P2PE

PCI DSS applies to all entities involved in payment card processing, and any entity that stores, processes, or transmits account data

- Covers security for any system components included in or connected to a merchant's or service provider's cardholder data environment (CDE)

PA-DSS and PCI DSS

- Payment applications must facilitate and not prevent PCI DSS compliance
- Many payment application requirements in PA-DSS address equivalent PCI DSS requirements

P2PE and PCI DSS

- Incorporates requirements from PTS, PCI DSS, PA-DSS, and PCI PIN to protect account data from the point of capture until it reaches the payment processor
- When properly implemented and maintained, Council-listed P2PE solutions may help reduce work involved during a merchant's PCI DSS assessment

PCI PIN Security Requirements

- These requirements provide for secure PIN:
  - management
  - processing
  - transmission
- Protection of personal identification number (PIN) data during online and offline payment card transaction processing at:
  - ATMs
  - attended point-of-sale (POS) terminals
  - unattended point-of-sale (POS) terminals
- The requirements also provide guidance on key management and key handling associated with the PIN

PCI PTS

- PTS requirements apply to: Point of Interaction (POI) devices; Encrypting PIN Pads (EPP); Point of Sale devices (POS); Hardware (or host) Security Modules (HSMs); Unattended Payment Terminals, (UPTs) and non-PIN Entry module
- The PTS program ensures terminals cannot be manipulated or attacked to allow the capture of Sensitive Authentication data, nor allow access to clear-text PINs or Keys
- The Secure Read and Exchange Module, (SRED) allows terminals to be approved for the secure encryption of cardholder data as part of the Point to Point Encryption program
- PTS has been extended to allow non-PIN entry modules to be evaluated against the SRED module to allow secure encryption at the point of interaction for non-chip and PIN cards

PCI DSS and PCI PTS Standards

PCI PTS - POI and PCI DSS

- PCI DSS requires that account data be protected both when stored and when transmitted across open, public networks
- PCI PTS POI validates how POIs protect PIN and account data and manage cryptographic keys
- PCI PTS POI-approved devices may form part of a PCI DSS-compliant environment

PCI PTS - PIN Security Standard and PCI DSS

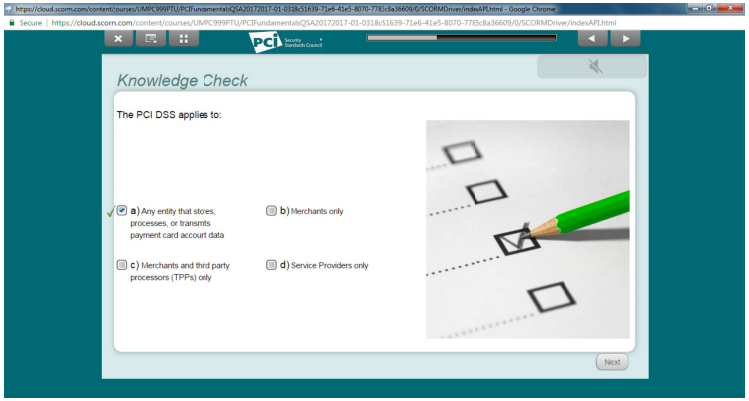
- PCI DSS prohibits storage of encrypted PIN blocks
- No overlap

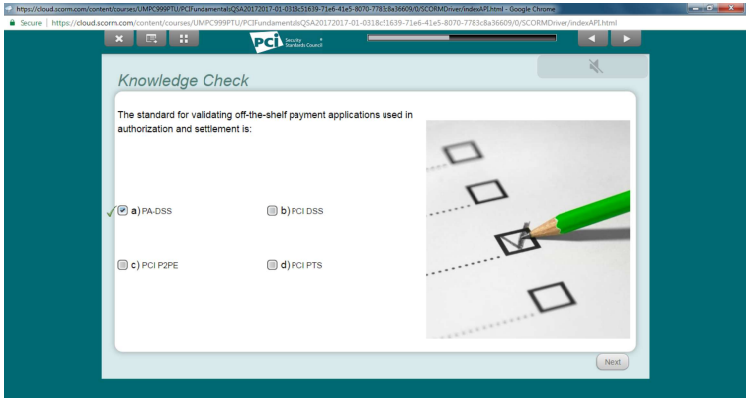
PCI Card Production and PCI DSS

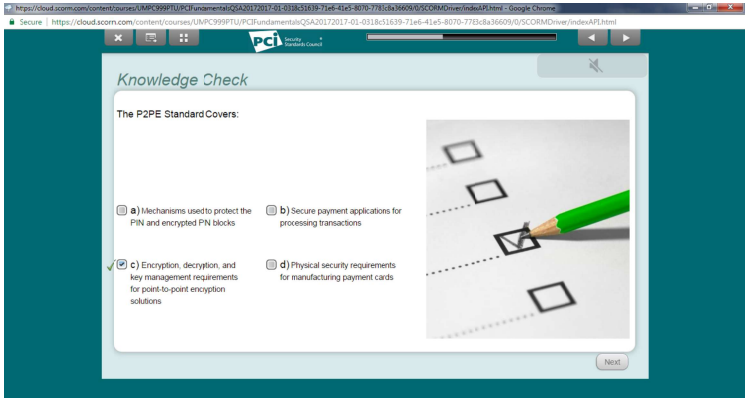
- No overlap
- Procedures for assessing card production facilities are defined and managed by the payment brands, not by PCI SSC

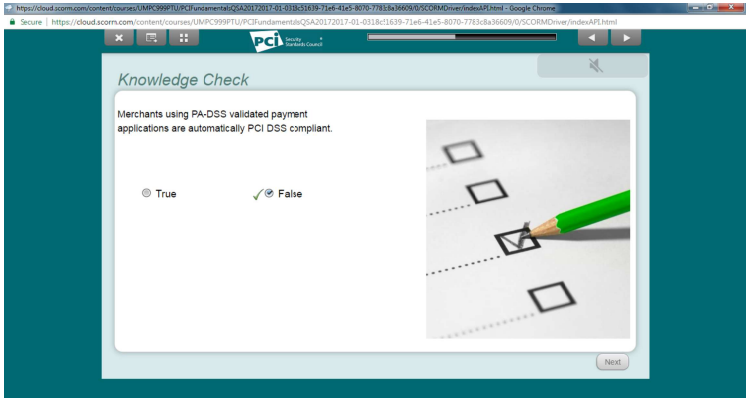
PCI PTS - HSM and PCI DSS

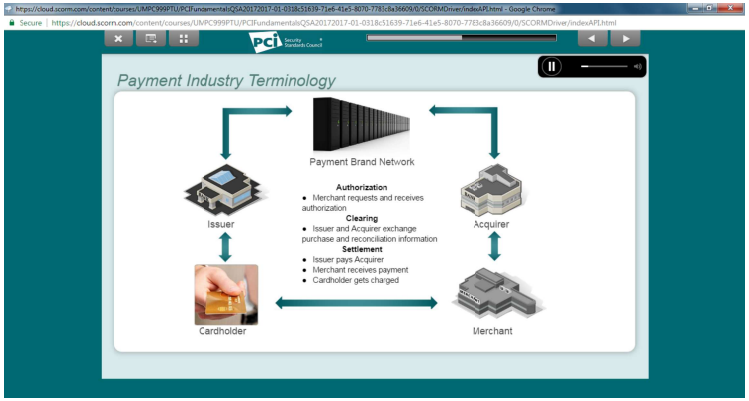
- PCI DSS requires that stored cardholder data be protected and cryptographic keys be managed in a secure manner
- Use of a Hardware Security Module is not required by PCI DSS, but may help with handling and managing keys used to protect stored cardholder data

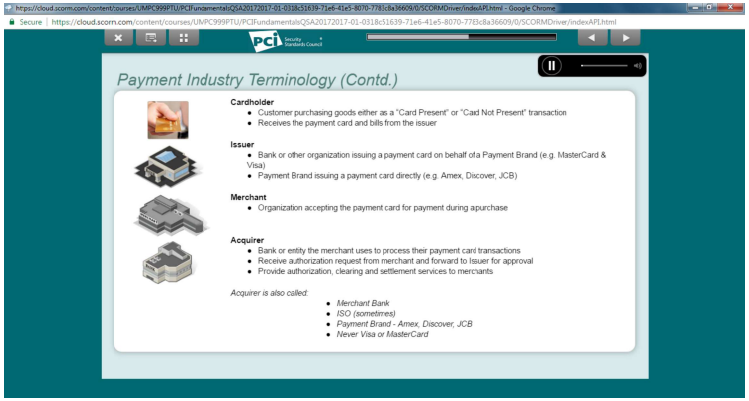

Knowledge Check
The PCI DSS applies to:
a) Any entity that stores, processes, or transmits payment card account data
b) Merchants only
c) Merchants and third party processors (TPPs) only
d) Service Providers only
Next

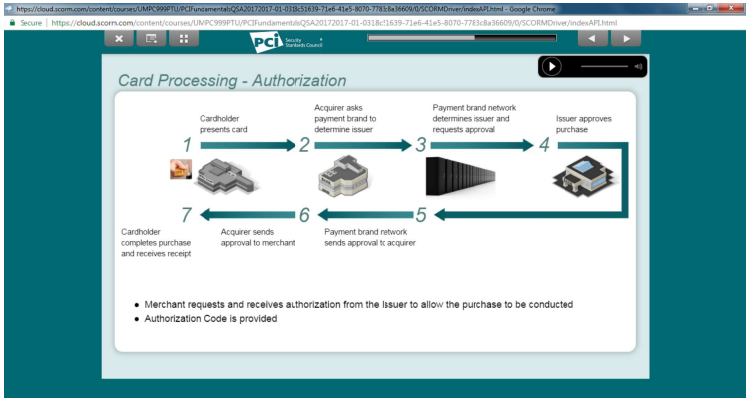

Knowledge Check
The standard for validating off-the-shelf payment applications used in authorization and settlement is:
a) PA-DSS
b) PCI DSS
c) PCI P2PE
d) PCI PTS
Next

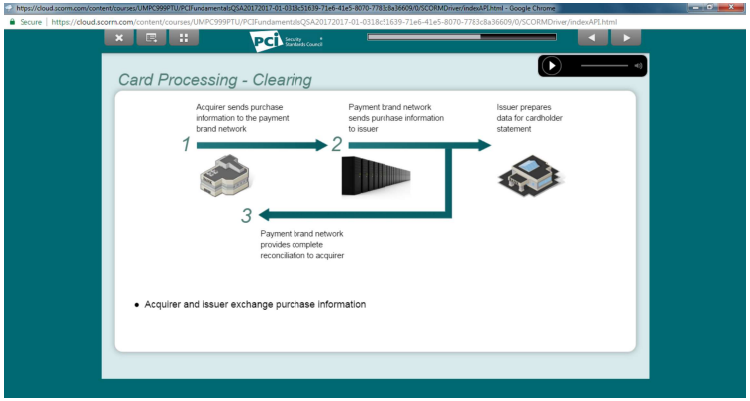

Knowledge Check
The P2PE Standard Covers:
a) Mechanisms used to protect the PIN and encrypted PIN blocks
b) Secure payment applications for processing transactions
c) Encryption, decryption, and key management requirements for point-to-point encryption solutions
d) Physical security requirements for manufacturing payment cards
Next

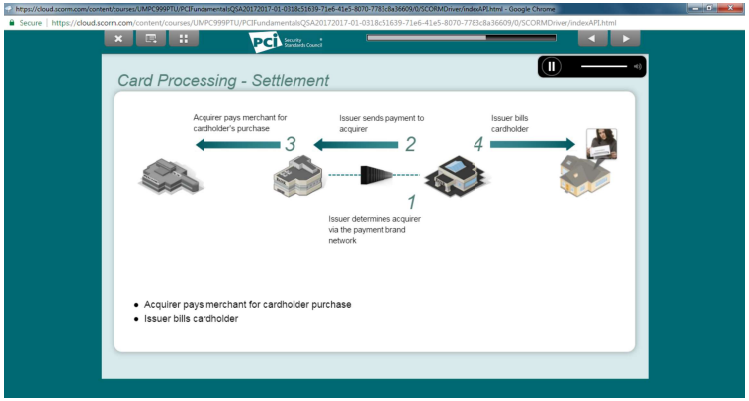

Knowledge Check
Merchants using PA-DSS validated payment applications are automatically PCI DSS compliant.
True
False
Next

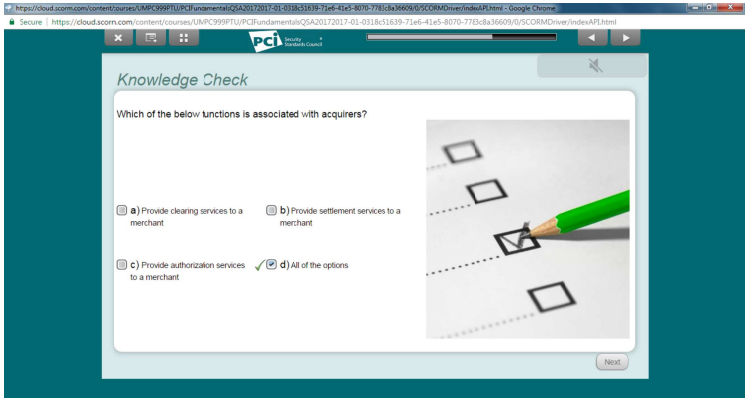

Payment Industry Terminology
Payment Brand Network
Issuer
Acquirer
Cardholder
Merchant
Authorization
Merchant requests and receives authorization
Clearing
Issuer and Acquirer exchange purchase and reconciliation information
Settlement
Issuer pays Acquirer
Merchant receives payment
Cardholder gets charged

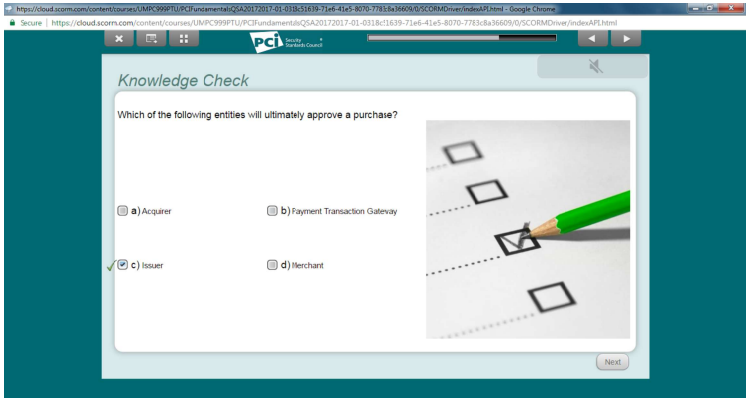

Payment Industry Terminology (Contd.)
Cardholder
Customer purchasing goods either as a "Card Present" or "Cad Not Present" transaction
Receives the payment card and bills from the issuer
Issuer
Bank or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa)
Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)
Merchant
Organization accepting the payment card for payment during apurchase
Acquirer
Bank or entity the merchant uses to process their payment card transactions
Receive authorization request from merchant and forward to Issuer for approval
Provide authorization, clearing and settlement services to merciants
Acquirer is also called:
Merchant Bank
ISO (sometimes)
Payment Brand - Amex, Discover, JCB
Never Visa or MasterCard

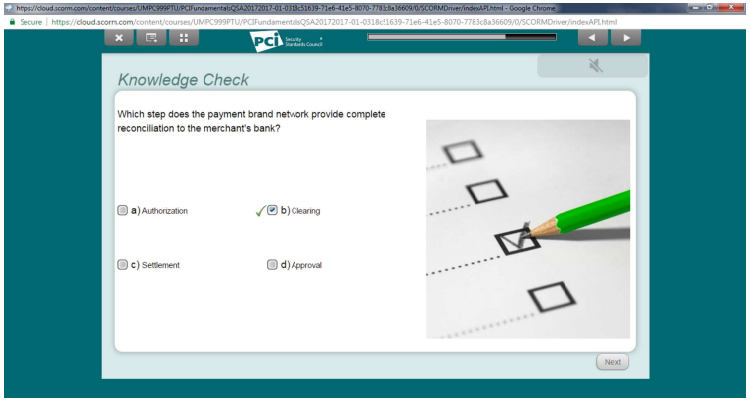

Card Processing - Authorization
Cardholder presents card
Acquirer asks payment brand to determine issuer
Payment brand network determines issuer and requests approval
Issuer approves purchase
1
2
3
4
5
6
7
Cardholder completes purchase and receives receipt
Acquirer sends approval to merchant
Payment brand network sends approval tc acquirer
Merchant requests and receives authorization from the Issuer to allow the purchase to be conducted
Authorization Code is provided


Card Processing - Clearing
Acquirer sends purchase information to the payment brand network
Payment brand network sends purhase information to issuer
Issuer prepares data for cardholder statement
1
2
3
Payment brand network provides complete reconciliation to acquirer
Acquirer and issuer exchange purchase information


Card Processing - Settlement
Acquirer pays merchant for cardholder's purchase
Issuer sends payment to acquirer
Issuer bills cardholder
3
2
4
1
Issuer determines acquirer via the payment brand network
Acquirer pays merchant for cardholder purchase
Issuer bills cardholder


Knowledge Check
Which of the below functions is associated with acquirers?
a) Provide clearing services to a merchant
b) Provide settlement services to a merchant
c) Provide authorization services to a merchant
d) All of the options
Next


Knowledge Check
Which of the following entities will ultimately approve a purchase?
a) Acquirer
b) Payment Transaction Gateway
c) Issuer
d) Merchant
Next


Knowledge Check
Which step does the payment brand network provide complete reconciliation to the merchant's bank?
a) Authorization
b) Clearing
c) Settlement
d) Approval
Next

Service Providers

A service provider is a business that is not a payment brand, directly involved in the processing, storage or transmission of cardholder data on behalf of another entity.

- Sometimes a service provider is a merchant

Includes companies that provide services (to merchants, service providers or other entities) which control or could impact the security of cardholder data.

Working with Service Providers

Entities often use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components of their CDE.

- There are two options for third-party service providers to validate compliance:
  - 1 - Undergo a PCI DSS assessment on their own and provide evidence to their customers demonstrating their compliance; or
  - 2 - Have their services reviewed during the course of each of their customers' PCI DSS assessments
- It's important to understand where the service provider's scope begins and ends for PCI DSS, for example:
  - The service(s) included in the service provider's PCI DSS validation
  - The PCI DSS requirements covered by the service provider's PCI DSS validation
- Any PCI DSS requirements related to the service which are the responsibility of the service provider's customers to maintain
  - The date of the service provider's last PCI DSS validation
  - The type and frequency of evidence provided by the service provider to their customers will depend on the agreement between those parties
  - Entities must monitor the PCI DSS compliance of their third-party service providers per PCI DSS Requirement 12.8

Knowledge Check

A company that _____ is considered to be a service provider.

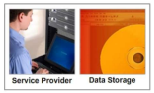
- [ ] a) Is a payment card brand
- [ ] b) Is not also a merchant
- [x] c) Controls or could impact the security of another entity's cardholder data
- [ ] d) Is a founding member of PCI SSC

Next

Service Provider Examples

Typical examples of service providers include:

- Transaction Processors
- Payment Gateways
- Independent Sales Organizations (ISOs) or External Sales Agents (ESAs)
- Customer Service functions
- Remittance processing companies
- Managed firewall and IDS service providers
- Web Hosting and Data Center Hosing providers
- Offsite data storage facilities



Some providers may not be included, for example:

- An entity that provides only public network access (such as a telecommunications company providing just the communication link)
- In this example, the entity using the communication link is responsible for securing transmissions of data over that link

Service Provider Examples (Contd.)

PCI DSS requirements for service providers will vary depending on the service being provided and the agreement between the provider and their customers. For example, consider the following scenarios:

- Companies that receive encrypted cardholder data but never have access to the encryption/decryption keys—for example, tape storage service provider with encrypted data
- Managed hosting providers providing IP addresses to their customers

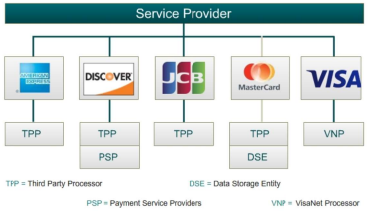
Knowledge Check

Which of the following are examples of service providers? (choose all that apply)

- a) Telecom providers (only communications link)
- ✓ b) Payment Gateways
- ✓ c) ISOs
- ✓ d) Data Center hosting providers

Next

Service Provider Terms



TPP = Third Party Processor

DSE = Data Storage Entity

PSP = Payment Service Providers

VNP = VisaNet Processor

Module Summary

In this module, we discussed the following aspects of the PCI DSS Compliance program:

- The Payment Card Industry Security Standards Council
- The Payment Card Industry Security Standards
- Payment Card Industry terminology
- The processes involved in card processing:
  - Authorization, Clearing, and Settlement
- Service provider relationships

Module Overview and Objectives

Module Topics:

- Payment Brand Compliance Programs
- SAQ Overview
- PA-DSS Overview
- Qualified Integrator/Reseller (QIR)
- P2PE Overview
- PCI Roles and Responsibilities

Module Objectives:

After completing this module, you will be able to:

- Describe payment brand compliance programs
- Define Levels and Transacton Volume
- Outline the Self-Assessmert Questionnaire and its various types
- State the key features of the Payment Application Data Security Standard
- Identify the applicability of PA-DSS to various payment applications
- Understand the role of QIRs
- Describe the roles and responsibilities of the PCI SSC and its members (Payment Brands)
- Describe the roles and responsibilities of the following:
  - Qualified Security Assessors (QSAs)
  - Merchants and Service Providers
  - Internal Security Assesors (ISAs)
  - Approved Scanning Vendors (ASVs)
  - Payment Application Qualified Security Assessors (PA-QSAs)

Payment Brand Compliance Programs

Payment brands' compliance programs include:

- Tracking and enforcement
- Penalties, fees, compliance deadlines
- Validation process and who needs to validate
- Approval and posting of compliant entities
- Definition of merchant and service provider levels

Payment brands are also responsible for:

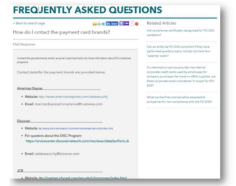
- Defining rules for forensic investigations and responding to account data compromises
- Monitoring and facilitating investigations of account data compromises to completion

The Founding Payment Brands

- Each payment brand develops and maintains its own PCI DSS compliance programs in accordance with its own security risk management policies.

American Express:	Data Security Operating Policy (DSOP)
Discover:	Discover Information Security Compliance (DISC)
JCB:	Data Security Program
MasterCard:	Site Data Protection (SDP)
Visa Inc.: Visa Europe:	Cardholder Information Security Program (CISP) Account Information Security (AIS) Program

Websites/Email for Additional Brand Information



Read FAQ 1142 on the SSC's website for a full list of contact details for the payment brands

Knowledge Check

Which of the following are parts of the Payment Brand role?
(Select all that apply)

- [x] a) Accept validation documentation from QSAs, PA-QSAs and ASVs
- [ ] b) Offer training for QSAs, PA-QSAs and ASVs
- [x] c) Endorse QSA, PA-QSA and ASV company qualification criteria
- [x] d) Develop and enforce compliance programs

Next

PCI DSS Validation Levels

Merchant Levels:

- Defined by the payment brands, based on transaction volume
- Transaction volume determined by the acquirer

Service Provider Levels:

- Defined by the payment brands according to transaction volume and/or type of service provider
- Determined by the payment brands or acquirer, or sometimes the service provider

Compliance validation requirements vary by payment brand.

PCI DSS Validation Requirements Overview

	Merchants		
	Level 1	**Level 2**	**Level 3 & 4**
Type of Assessment:	Onsite Assessment	Self-assessment	Determined by Payment Brand or Acquirer
Reporting Requirements:	ROC and ASV Scan Report	SAQ and ASV Scan Report	Determined by Payment Brand or Acquirer

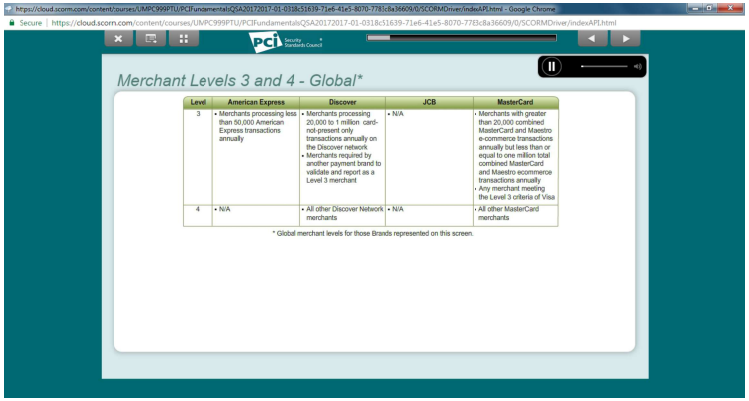
	Service Providers		
	Level 1	**Level 2**	**Level 3 (American Express)**
Type of Assessment:	Onsite Assessment	Self-Assessment	Self-Assessment
Reporting Requirements:	ROC and ASV Scan Report	SAQand ASV Scan Report	SAQ and ASV Scan Report

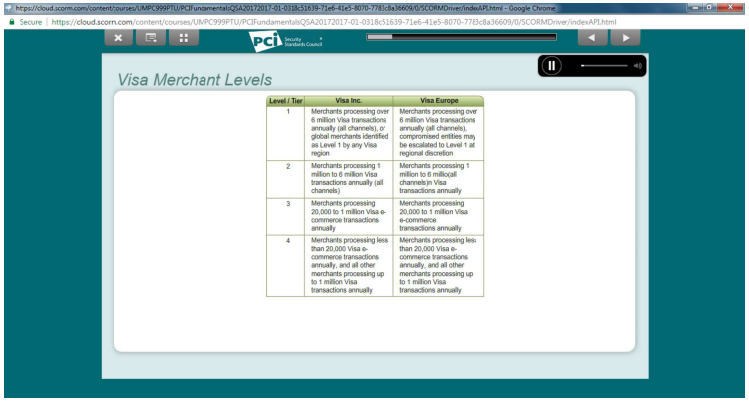
**This is a summarized overview only - Merchants and Service Providers should consult with their acquirer or payment brand directly to understand each brand's validation criteria and reporting requirements.*

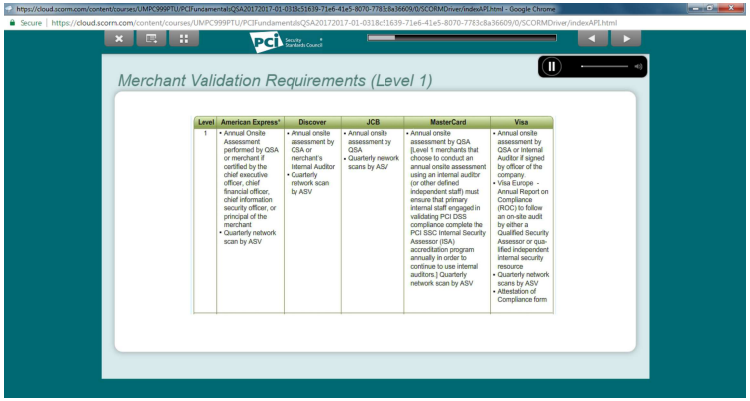
Merchant Levels 1 and 2– Global*

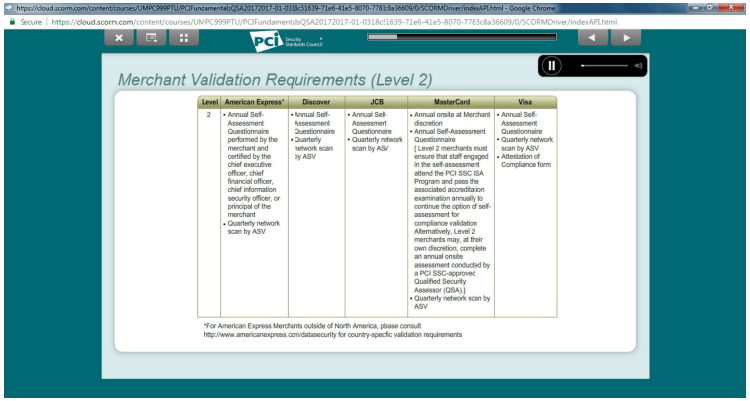
Level	American Express	Discover	JCB	MasterCard
1	• Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express otherwise deems a Level 1	• Merchants processing over 6 million card transactions annually on the Discover network • Any merchant Discover determines to be a Level 1 • Merchants required by another payment brand to validate and report as a Level 1	• Merchants processing over 1 million JCB transactions annually, or compromised merchants	• Merchants processing over 6 million total combined MasterCard and Maestro transactions annually • Merchants that have experienced an account data compromise • Any merchant that MasterCard otherwise deems a Level 1 • Any merchant meeting the Level 1 criteria of Visa
2	• Merchants processing 50,000 to 2.5 million American Express transactions annually	• Merchants processing 1 million to 6 million card transactions annually on the Discover network • Merchants required by another payment brand to validate and report as a Level 2 merchant	• Merchants processing less than 1 million JCB transactions annually	• Merchants with greater than 1 million but less than or equal to 6 million total combined MasterCard and Maestro transactions annually • Any merchant meeting the Level 2 criteria of Visa

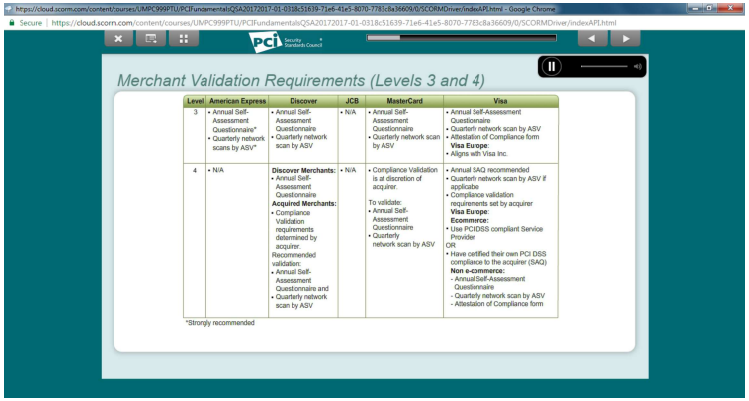
* Global merchant levels for those Brands represented on this screen.

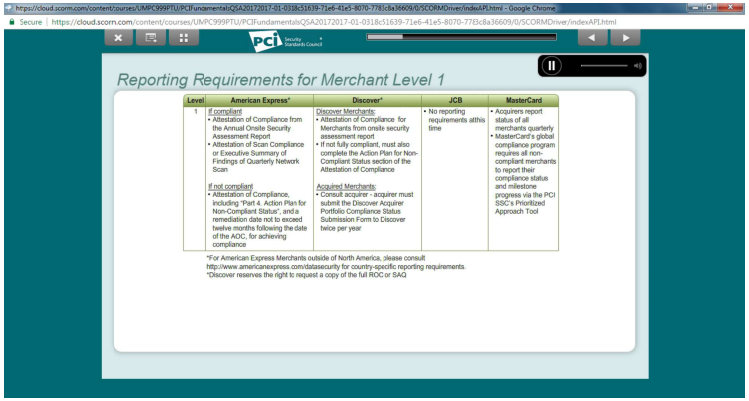

Merchant Levels 3 and 4 - Global*
Level
American Express
Discover
JCB
MasterCard
3
• Merchants processing less than 50,000 American Express transactions annually
• Merchants processing 20,000 to 1 million card-not-present only transactions annually on the Discover network
• Merchants required by another payment brand to validate and report as a Level 3 merchant
• N/A
• Merchants with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro ecommerce transactions annually
• Any merchant meeting the Level 3 criteria of Visa
4
• N/A
• All other Discover Network merchants
• N/A
• All other MasterCard merchants
* Global merchant levels for those Brands represented on this screen.

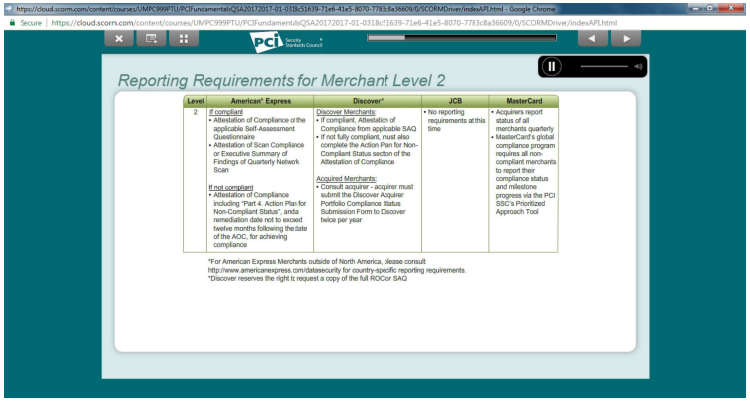

Visa Merchant Levels
Level / Tier
Visa Inc.
Visa Europe
1
Merchants processing over 6 million Visa transactions annually (all channels), or global merchants identified as Level 1 by any Visa region
Merchants processing over 6 million Visa transactions annually (all channels), compromised entities may be escalated to Level 1 at regional discretion
2
Merchants processing 1 million to 6 million Visa transactions annually (all channels)
Merchants processing 1 million to 6 millio(all channels)n Visa transactions annually
3
Merchants processing 20,000 to 1 million Visa e-commerce transactions annually
Merchants processing 20,000 to 1 million Visa e-commerce transactions annually
4
Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually
Merchants processing less than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to 1 million Visa transactions annually

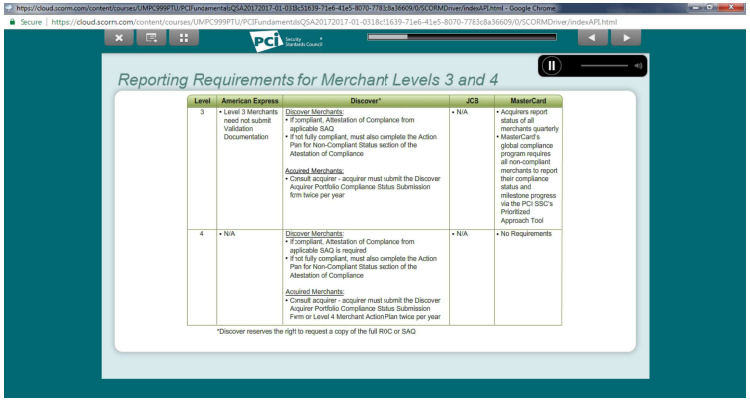

Merchant Validation Requirements (Level 1)
Level
American Express*
Discover
JCB
MasterCard
Visa
1
• Annual Onsite Assessment performed by QSA or merchant if certified by the chief executive officer, chief financial officer, chief information security officer, or principal of the merchant
• Quarterly network scan by ASV
• Annual onsite assessment by CSA or nerchant's Internal Auditor
• Quarterly network scan by ASV
• Annual onsite assessment by QSA
• Quarterly network scans by ASV
• Annual onsite assessment by QSA [Level 1 merchants that choose to conduct an annual onsite assessment using an internal auditor (or other defined independent staff) must ensure that primary internal staff engaged in validating PCI DSS compliance complete the PCI SSC Internal Security Assessor (ISA) accreditation program annually in order to continue to use internal auditors.] Quarterly network scan by ASV
• Annual onsite assessment by QSA or Internal Auditor if signed by officer of the company
• Visa Europe - Annual Report on Compliance (ROC) to follow an on-site audit by either a Qualified Security Assessor or qua-lified independent internal security resource
• Quarterly network scans by ASV
• Attestation of Compliance form

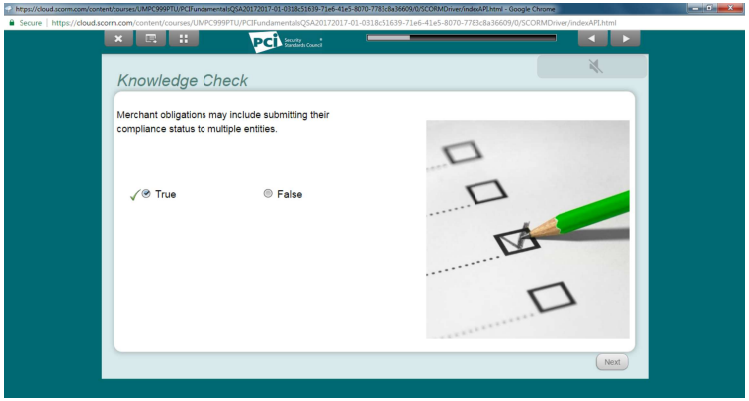

Merchant Validation Requirements (Level 2)
Level
American Express*
Discover
JCB
MasterCard
Visa
2
• Annual Self-Assessment Questionnaire performed by the merchant and certified by the chief executive officer, chief financial officer, chief information security officer, or principal of the merchant
• Quarterly network scan by ASV
• Annual Self-Assessment Questionnaire
• Quarterly network scan by ASV
• Annual Self-Assessment Questionnaire
• Quarterly network scan by ASV
• Annual onsite at Merchant discretion
• Annual Self-Assessment Questionnaire [Level 2 merchants must ensure that staff engaged in the self-assessment attend the PCI SSC ISA Program and pass the associated accreditation examination annually to continue the option of self-assessment for compliance validation Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC-approvec Qualified Security Assessor (QSA).]
• Quarterly network scan by ASV
• Annual Self-Assessment Questionnaire
• Quarterly network scan by ASV
• Attestation of Compliance form
*For American Express Merchants outside of North America, please consult http://www.americanexpress.com/datasecurity for country-specific validation requirements

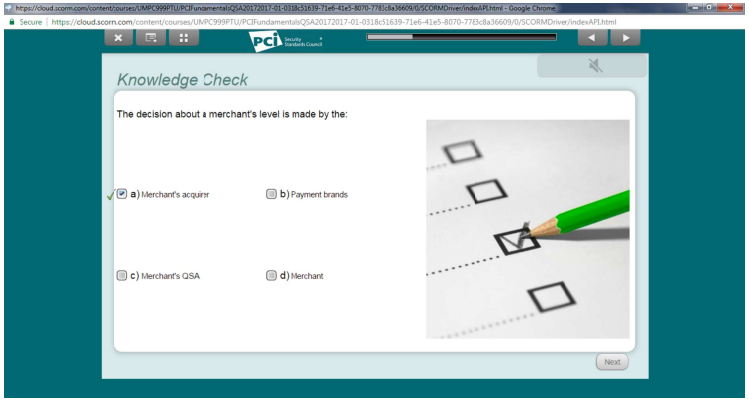

Merchant Validation Requirements (Levels 3 and 4)
Level | American Express | Discover | JCB | MasterCard | Visa
3 | • Annual Self-Assessment Questionnaire* • Quarterly network scans by ASV* | • Annual Self-Assessment Questionnaire • Quarterly network scan by ASV | • N/A | • Annual Self-Assessment Questionnaire • Quarterly network scan by ASV | • Annual Self-Assessment Questionnaire • Quarterly network scan by ASV • Attestation of Compliance form Visa Europe: • Aligns with Visa Inc.
4 | • N/A | Discover Merchants: • Annual Self-Assessment Questionnaire Acquired Merchants: • Compliance Validation requirements determined by acquirer. Recommended validation: • Annual Self-Assessment Questionnaire and • Quarterly network scan by ASV | • N/A | • Compliance Validation is at discretion of acquirer. To validate: • Annual Self-Assessment Questionnaire • Quarterly network scan by ASV | • Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer Visa Europe: Ecommerce: • Use PCIDSS compliant Service Provider OR • Have certified their own PCI DSS compliance to the acquirer (SAQ) Non e-commerce: - AnnualSelf-Assessment Questinnaire - Quarterly network scan by ASV - Attestation of Compliance form
*Strongly recommended

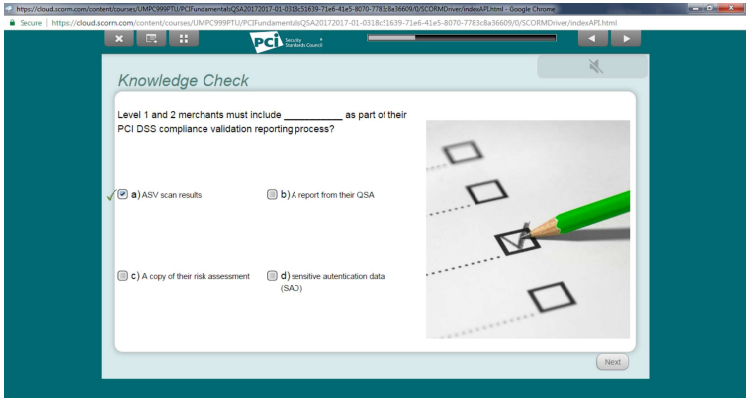

Reporting Requirements for Merchant Level 1
Level | American Express* | Discover* | JCB | MasterCard
1 | If compliant • Attestation of Compliance from the Annual Onsite Security Assessment Report • Attestation of Scan Compliance or Executive Summary of Findings of Quarterly Network Scan If not compliant • Attestation of Compliance, including "Part 4. Action Plan for Non-Compliant Status", and a remediation date not to exceed twelve months following the date of the AOC, for achieving compliance | Discover Merchants: • Attestation of Compliance for Merchants from onsite security assessment report • If not fully compliant, must also complete the Action Plan for Non-Compliant Status section of the Attestation of Compliance Acquired Merchants: • Consult acquirer - acquirer must submit the Discover Acquirer Portfolio Compliance Status Submission Form to Discover twice per year | • No reporting requirements atthis time | • Acquirers report status of all merchants quarterly • MasterCard's global compliance program requires all non-compliant merchants to report their compliance status and milestone progress via the PCI SSC's Prioritized Approach Tool
*For American Express Merchants outside of North America, please consult http://www.americanexpress.com/datasecurity for country-specific reporting requirements.
*Discover reserves the right tc request a copy of the full ROC or SAQ

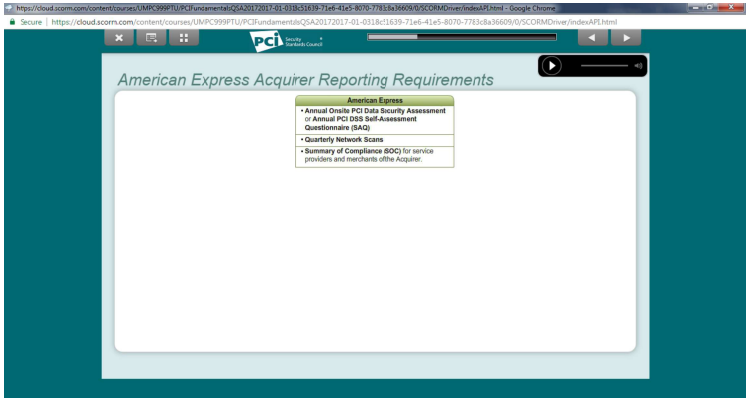

Reporting Requirements for Merchant Level 2
Level | American* Express | Discover* | JCB | MasterCard
2 | If compliant • Attestation of Compliance of the applicable Self-Assessment Questionnaire • Attestation of Scan Compliance or Executive Summary of Findings of Quarterly Network Scan If not compliant • Attestation of Compliance including "Part 4. Action Plan for Non-Compliant Status", anda remediation date not to exceed twelve months following the date of the AOC, for achieving compliance | Discover Merchants: • If compliant, Attestatio of Compliance from applicable SAQ • If not fully compliant, must also complete the Action Pan for Non-Compliant Status section of the Attestation of Compliance Acquired Merchants: • Consult acquirer - acquirer must submit the Discover Acquirer Portfolio Compliance Status Submission Form to Discover twice per year | • No reporting requirements at this time | • Acquirers report status of all merchants quarterly • MasterCard's global compliance program requires all non-compliant merchants to report their compliance status and milestone progress via the PCI SSC's Prioritized Approach Tool
*For American Express Merchants outside of North America, lease consult http://www.americanexpress.com/datasecurity for country-specific reporting requirements.
*Discover reserves the right tc request a copy of the full ROCor SAQ


Reporting Requirements for Merchant Levels 3 and 4
Level | American Express | Discover* | JCB | MasterCard
3 | • Level 3 Merchants need not submit Validation Documentation | Discover Merchants: • If compliant, Attestation of Compliance from applicable SAQ • If not fully compliant, must also complete the Action Pan for Non-Compliant Status section of the Attestation of Compliance Acquired Merchants: • Consult acquirer - acquirer must submit the Discover Acquirer Portfolio Compliance Status Submission form twice per year | • N/A | • Acquirers report status of all merchants quarterly • MasterCard's global compliance program requires all non-compliant merchants to report their compliance status and milestone progress via the PCI SSC's Prioritized Approach Tool
4 | • N/A | Discover Merchants: • If compliant, Attestation of Compliance from applicable SAQ is required • If not fully compliant, must also complete the Action Pan for Non-Compliant Status section of the Attestation of Compliance Acquired Merchants: • Consult acquirer - acquirer must submit the Discover Acquirer Portfolio Compliance Status Submission Form or Level 4 Merchant ActionPlan twice per year | • N/A | • No Requirements
*Discover reserves the right to request a copy of the full ROC or SAQ


Knowledge Check
Merchant obligations may include submitting their compliance status tc multiple entities.
True
False
Next


Knowledge Check
The decision about a merchant's level is made by the:
a) Merchant's acquirer
b) Payment brands
c) Merchant's QSA
d) Merchant
Next


Knowledge Check
Level 1 and 2 merchants must include _____ as part of their PCI DSS compliance validation reporting process?
a) ASV scan results
b) A report from their QSA
c) A copy of their risk assessment
d) ensitive autentication data (SAO)
Next


American Express Acquirer Reporting Requirements
American Express
• Annual Onsite PCI Data Scurity Assessment or Annual PCI DSS Self-Asessment Questionnaire (SAQ)
• Quarterly Network Scans
• Summary of Compliance (SOC) for service providers and merchants ofthe Acquirer.

Visa Acquirer Reporting Requirements

Level/ Tier	Visa Inc.	Visa Europe
1	• At least twice a year, a statement of merchant compliance/non-compliance • Annual Attestation of Compliance form • Upon request, a copy of ROC	• Quarterly statement of merchant compliance/non-compliance for all merchants • Upon request, a copy of ROC (including indication of scan completion)
2	• At least twice a year, a statement of merchant compliance/non-compliance • Annual Attestation of Compliance form • Upon request, a copy of SAQ	• Quarterly statement of merchant compliance/non-compliance for all merchants • Upon request, a copy of SAQ and AOC
3	• At least twice a year, statement of compliance/ non-compliance	• Quarterly statement of merchant compliance/non-compliance for all merchants • Upon request, a copy of SAQ and AOC
4	• Set by acquirer	• Quarterly statement of merchant compliance/non-compliance for all merchants • Upon request, a copy of SAQ and AOC for e-commerce merchants

Service Provider Levels

Level	American Express
1	• Service Providers processing over 2.5 million American Express Card transactions annually or any service provider that American Express otherwise deems a Level 1
2	• Service Providers processing 50,000 to 2.5 million American Express transactions annually
3	• Service Providers processing less than 50,000 American Express transactions annually

Service Provider Levels

American Express, Discover, MasterCard, and Visa

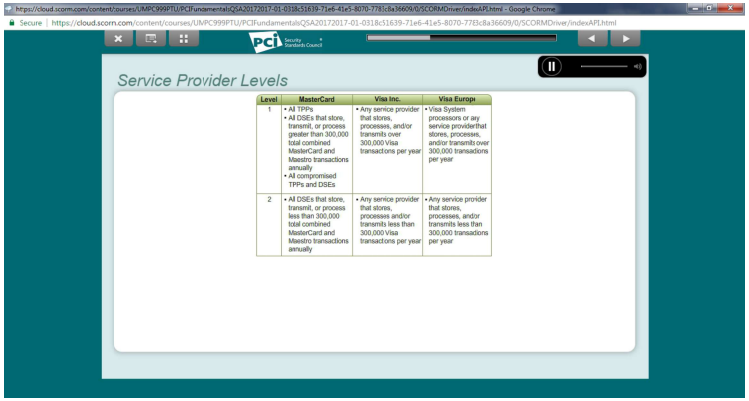
- Categorize service providers according to transaction volume and/or type of service provider
- PCI DSS compliance validation and reporting is defined according to the service provider level

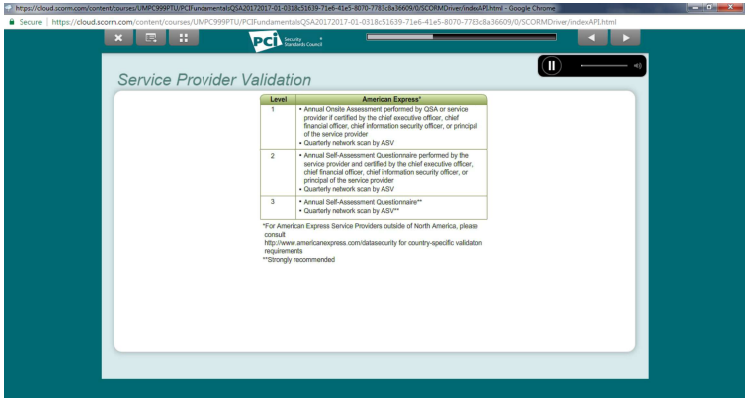
JCB International

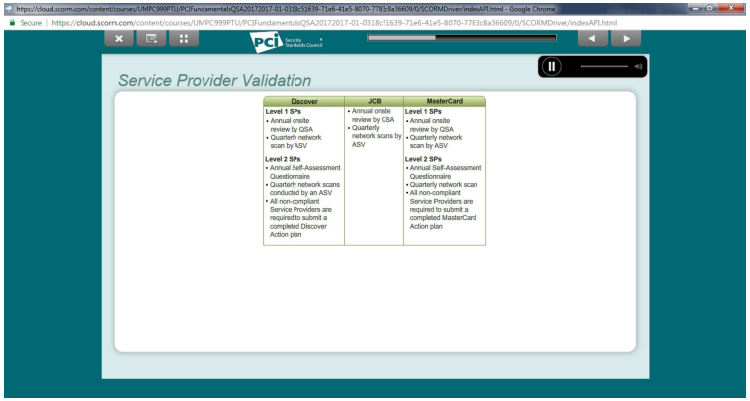
- Service providers include all third party processors regardless of transaction volume

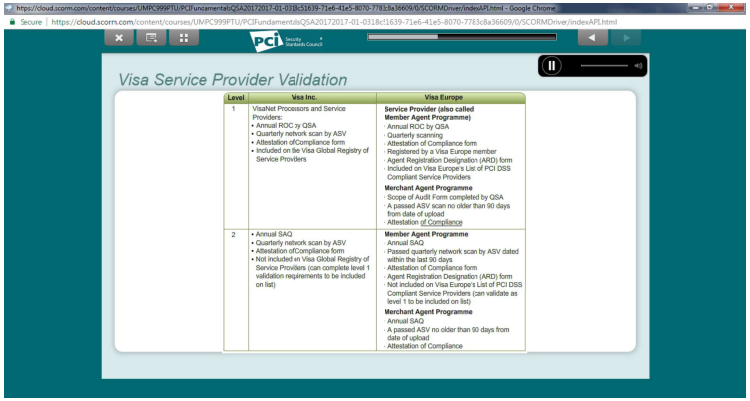
Service Provider Levels

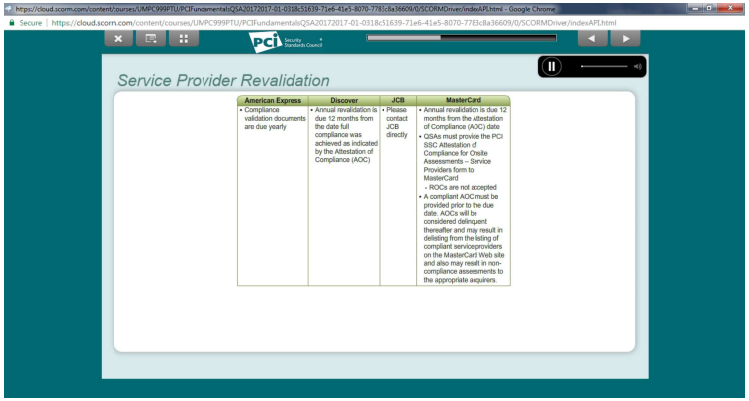
Level	Discover	JCB
1	• All Service Providers that store, process, and/or transmit over 300,00(Discover Network card transactions per year • Any Service Provider that Discover, in its sole discretion, determines should meet the Level 1 compliance validation and reporting requirements	• All TPPs
2	• All Service Providers that store, process, and/or transmit less than 30k,000 Discover Network card transactions per year	

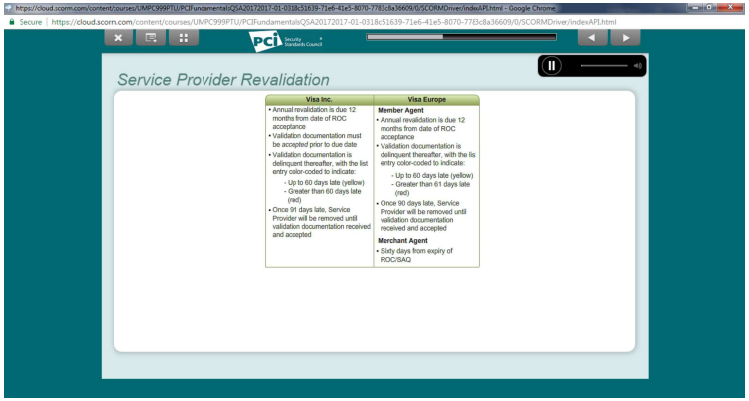

Service Provider Levels
Level
MasterCard
Visa Inc.
Visa Europe
1
• All TPPs
• All DSEs that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually
• All compromised TPPs and DSEs
• Any service provider that stores, processes, and/or transmits over 300,000 Visa transactions per year
• Visa System processors or any service providerthat stores, processes, and/or transmits over 300,000 transactions per year
2
• All DSEs that store, transmit, or process less than 300,000 total combined MasterCard and Maestro transactions annually
• Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions per year
• Any service provider that stores, processes, and/or transmits less than 300,000 transactions per year

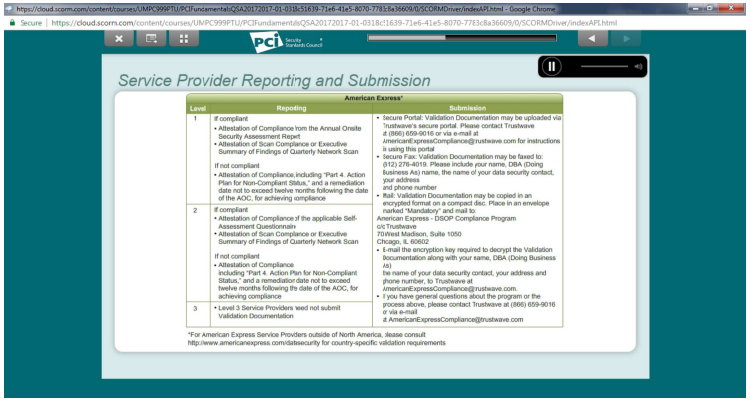

Service Provider Validation
Level
American Express*
1
• Annual Onsite Assessment performed by QSA or service provider if certified by the chief executive officer, chief financial officer, chief information security officer, or principal of the service provider
• Quarterly network scan by ASV
2
• Annual Self-Assessment Questionnaire performed by the service provider and certified by the chief executive officer, chief financial officer, chief information security officer, or principal of the service provider
• Quarterly network scan by ASV
3
• Annual Self-Assessment Questionnaire**
• Quarterly network scan by ASV**
*For American Express Service Providers outside of North America, please consult http://www.americanexpress.com/datasecurity for country-specific validaton requirements
**Strongly recommended

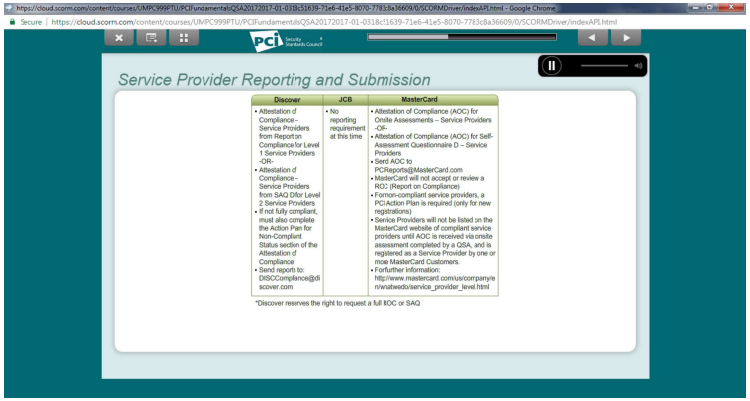

Service Provider Validation
Discover
Level 1 SPs
• Annual onsite review by QSA
• Quarterly network scan by ASV
Level 2 SPs
• Annual Self-Assessment Questionnaire
• Quarterly network scans conducted by an ASV
• All non-compliant Service Providers are requiredto submit a completed Discover Action plan
JCB
• Annual onsite review by CSA
• Quarterly network scans by ASV
MasterCard
Level 1 SPs
• Annual onsite review by QSA
• Quarterly network scan by ASV
Level 2 SPs
• Annual Self-Assessment Questionnaire
• Quarterly network scan
• All non-compliant Service Providers are required to submit a completed MasterCard Action plan


Visa Service Provider Validation
Level
Visa Inc.
Visa Europe
1
VisaNet Processors and Service Providers:
• Annual ROC by QSA
• Quarterly network scan by ASV
• Attestation ofCompliance form
• Included on the Visa Global Registry of Service Providers
Service Provider (also called Member Agent Programme)
· Annual ROC by QSA
· Quarterly scanning
· Attestation of Compliance form
· Registered by a Visa Europe member
· Agent Registration Designation (ARD) form
· Included on Visa Europe's List of PCI DSS Compliant Service Providers
Merchant Agent Programme
· Scope of Audit Form completed by QSA
· A passed ASV scan no older than 90 days from date of upload
· Attestation of Compliance
2
• Annual SAQ
• Quarterly network scan by ASV
• Attestation ofCompliance form
• Not included on Visa Global Registry of Service Providers (can complete level 1 validation requirements to be included on list)
Member Agent Programme
· Annual SAQ
· Passed quarterly network scan by ASV dated within the last 90 days
· Attestation of Compliance form
· Agent Registration Designation (ARD) form
· Not included on Visa Europe's List of PCI DSS Compliant Service Providers (can validate as level 1 to be included on list)
Merchant Agent Programme
· Annual SAQ
· A passed ASV no older than 90 days from date of upload
· Attestation of Compliance


Service Provider Revalidation
American Express
• Compliance validation documents are due yearly
Discover
• Annual revalidation is due 12 months from the date full compliance was achieved as indicated by the Attestation of Compliance (AOC)
JCB
• Please contact JCB directly
MasterCard
• Annual revalidation is due 12 months from the attestation of Compliance (AOC) date
• QSAs must provide the PCI SSC Attestation of Compliance for Onsite Assessments – Service Providers form to MasterCard
- ROCs are not accepted
• A compliant AOCmust be provided prior to he due date. AOCs will be considered delinquent thereafter and may result in delisting from the listing of compliant serviceproviders on the MasterCard Web site and also may result in non-compliance assesments to the appropriate aquirers.


Service Provider Revalidation
Visa Inc.
• Annual revalidation is due 12 months from date of ROC acceptance
• Validation documentation must be accepted prior to due date
• Validation documentation is delinquent thereafter, with the list entry color-coded to indicate:
- Up to 60 days late (yellow)
- Greater than 60 days late (red)
• Once 91 days late, Service Provider will be removed until validation documentation received and accepted
Visa Europe
Member Agent
• Annual revalidation is due 12 months from date of ROC acceptance
• Validation documentation is delinquent thereafter, with the lis entry color-coded to indicate:
- Up to 60 days late (yellow)
- Greater than 61 days late (red)
• Once 90 days late, Service Provider will be removed until validation documentation received and accepted
Merchant Agent
• Sixty days from expiry of ROC/SAQ


Service Provider Reporting and Submission
American Express*
Level
Repoting
Submission
1
If compliant
• Attestation of Compliance from the Annual Onsite Security Assessment Report
• Attestation of Scan Compliance or Executive Summary of Findings of Quarterly Network Scan
If not compliant
• Attestation of Compliance,including "Part 4. Action Plan for Non-Compliant Status," and a remediation date not to exceed twelve months following the date of the AOC, for achieving compliance
• Secure Portal: Validation Documentation may be uploaded via Trustwave's secure portal. Please contact Trustwave at (866) 659-9016 or via e-mail at AmericanExpressCompliance@trustwave.com for instructions in using this portal
• Secure Fax: Validation Documentation may be faxed to: (312) 276-4019. Please include your name, DBA (Doing business As) name, the name of your data security contact, your address and phone number
• Mail: Validation Documentation may be copied in an encrypted format on a compact disc. Place in an envelope marked "Mandatory" and mail to:
American Express - DSOP Compliance Program
c/o Trustwave
70West Madison, Suite 1050
Chcago, IL 60602
• E-mail the encryption key required to decrypt the Validation documentation along with your name, DBA (Doing Business As)
the name of your data security contact, your address and phone number, to Trustwave at AmericanExpressCompliance@trustwave.com.
• f you have general questions about the program or the process above, please contact Trustwave at (866) 659-9016 or via e-mail at AmericanExpressCompliance@trustwave.com
2
If compliant
• Attestation of Compliance if the applicable Self-Assessment Questionnaire
• Attestation of Scan Compliance or Executive Summary of Findings of Quarterly Network Scan
If not compliant
• Attestation of Compliance including "Part 4. Action Plan for Non-Compliant Status," and a remediation date not to exceed twelve months following the date of the AOC, for achieving compliance
3
• Level 3 Service Providers need not submit Validation Documentation
*For American Express Service Providers outside of North America, please consult http://www.americanexpress.com/datasecurity for country-specific validation requirements

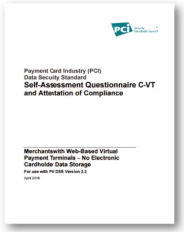

Service Provider Reporting and Submission
Discover
• Attestation of Compliance – Service Providers from Reporton Compliance for Level 1 Service Providers
-OR-
• Attestation of Compliance – Service Providers from SAQ Dfor Level 2 Service Providers
• If not fully compliant, must also complete the Action Pan for Non-Compliant Status sectin of the Attestation of Compliance
• Send reports to: DISCCompliance@discover.com
JCB
• No reporting requirement at this time
MasterCard
• Attestation of Compliance (AOC) for Onsite Assessments – Service Providers -OR-
• Attestation of Compliance (AOC) for Self-Assessment Questionnaire D – Service Providers
• Send AOC to PCIReports@MasterCard.com
• MasterCard will not accept or review a ROC (Report on Compliance)
• Fornon-compliant service providers, a PCI Action Plan is required (only for new registrations)
• Service Providers will not be listed on the MasterCard website of compliant service providers until AOC is received via onsite assessment completed by a QSA, and is registered as a Service Provider by one or moe MasterCard Customers.
• Forfurther information: http://www.mastercard.com/us/company/en/whatwedo/service_providar_level.html
*Discover reserves the right to request a full ROC or SAQ

Service Provider Reporting and Submission

Visa Inc.	Visa Europe
• Attestation of Compliance (Third Party Agents) and Full ROC and Attestation of Compliance (VisaNet Processors) must be submitted to Visa – send to pcimoz@visa.com and AP-CEMEA region send to pciagents@visa.com • Service providers MUST BE registered with Visa before being added to the Global Registry of Service Providers. For additional information send an e-mail to: Americas - AgentRegistration@visa.com AP-CEMEA - agents@visa.com • For Visa AP-CEMEA, visit www.visa.com/staysecureAPCEMEA for information about the Direct Registration Program. • The Visa Global Registry of Service Providers is published here: http://www.visa.com/splisting	• Service Providers (Member Agents) - ROC, QSA confirmation form Attestation of Compliance form etc. must be submitted to Visa – send to pcidsseurope@visa.com • Merchants Agents – Online submission via https://www.visamerchantagents.com/ • Service providers MUST BE registered with Visa by a Visa Europe Member before being added to list – email agentcompliance@visa.com for information • Visa Europe's List of Compliant Service Providers is published on the AIS website: http://www.visaeurope.com/en/businesses__retailers/payment_security.aspx

Self-Assessment Questionnaire (SAQ)

- The Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS
- There are multiple versions of the PCI DSS SAQ to meet various scenarios
- The PCI DSS SAQ is a validation tool for merchants and service providers not required to submit an on-site data security assessment Report on Compliance.


Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire C-VT and Attestation of Compliance

Merchantswith Web-Based Virtual Payment Terminals - No Electronic Cardholde Data Storage
For use with PCI DSS Version 3.2

Self-Assessment Questionnaire (SAQ) (Contd.)

SAQ	Description*
A	Card-Not-Present (e-commerce or MO/TO) merchants, all cardholder data functions outsourced to PCI DSS compliant service providers. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only stand-alone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

*Refer to "Before you Begin" section in each SAQ for full eligibility criteria

Self-Assessment Questionnaire (SAQ) (Contd.)

SAQ	Description*
C	Merchants with segmented payment application systems connected to the Internet, with no electronic cardholder data storage *Not applicable to e-commerce channels.*
C-VT	Merchants using only web-based virtual payment terminals, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	**SAQ D for Merchants**: All merchants not included in the descriptions for other SAQ types. **SAQ D for Service Providers**: All service providers identified by a payment brands as eligible to complete a self-assessment questionnaire.
P2PE	Merchants who have implemented a validated Point-to-Point Encryption Solution that is listed on the PCI SSC website, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

*Refer to "Before you Begin" section in each SAQ for full eligibility criteria

Knowledge Check

Which SAQ best applies to the entities below? (Assume that none of the entities store any cardholder data electronically)

Drag each SAQ onto the correct description

Service provider using only web-based virtual t… — SAQ D

MC/TO merchant with all payment functions outsourced… compliant service provider — SAQ A

Merchant with standa… ment application connecte… SAQ C …ternet

Merchant with only… sent dia-out terminals — SAQ B

Next

Knowledge Check

Which SAQ best applies to the entities below? (Assume that none of the entities store any cardholder data electronically)

Drag each SAQ onto the correct description

Merchant who is using a validated P2PE solution listed on the PCI SSC website. — SAQ P2PE

An online merchant with a payment page that accepts cardholder data… — SAQ A-EP

An online merchant that displays a PCI DSS-compliant service provider's payment page in… IFRAME, all page content… the PSP. — SAQ A

Merchant using an end-to-… encryption solution (E2EE)… utilises PCI PTS-approved… devices which communicate with the… acquirer over an IP network. — SAQ B-IP

Next

PA-DSS Overview

- PA-DSS is a comprehensive set of requirements designed for payment application software vendors to facilitate their customers' PCI DSS compliance
- Distinct from but aligned with PCI DSS
- PA-DSS applies to third-party payment applications that perform authorization and/or settlement

PA-DSS Applicability

PA-DSS applies to third-party payment applications

- If application performs authorization and/or settlement (POS, shopping carts, etc.)

PA-DSS ensures a payment application functions in a PCI DSS compliant manner

- To support the PCI DSS compliance of those that use the application
- Use of a PA-DSS application alone does not guarantee PCI DSS compliance

PA-DSS applications are in scope for PCI DSS Assessor must validate that payment application is installed:

- Per instructions in the PA-DSS Implementation Guide provided by payment application vendor
- In a PCI DSS compliant manner

Assessing Environments with PA-DSS Applications

- Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant
- PA-DSS validated payment applications are included in the scope of a PCI DSS assessment
- The assessor should not challenge the PA-DSS validation
- PCI DSS assessment of validated payment applications should verify:
  - The payment application is implemented into a PCI DSS compliant environment
  - The payment application is implemented according to the PA-DSS Implementation Guide
- All other system components in scope for PCI DSS must still be assessed
- The assessor should focus their assessment on the application's implementation in accordance with the vendor's implementation guide

Payment Brand Compliance Programs – PA-DSS

Each payment brand establishes their own PA-DSS compliance program including:

- Who/which application must comply
- Mandates
- Due dates
- Fines and penalties

PA-DSS Applicability

PA-DSS applies to payment applications that are typically sold and installed "off-the-shelf" without much customization by software vendors.

PA-DSS applies to payment applications provided in modules, which typically includes a "baseline" module and other modules specific to customer types or functions

- PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA)
- If other modules also perform payment functions, PA-DSS applies to those modules as well
- Note that it is considered a "best practice" for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions

PA-DSS Applicability

PA-DSS does not apply to a payment application developed for and sold to only one customer since this application will be covered as part of the customer's PCI DSS compliance review.

- Such an application (which may be referred to as a "bespoke" application) is sold to only one customer (for example, a large merchant or service provider), and it is designed and developed according to customer-provided specifications.

PA-DSS does not apply to payment applications developed by merchants and service providers if used only in-house (not sold to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's PCI DSS compliance.

PA-DSS Applicability

The following list illustrates applications that are not payment applications for purposes of PA-DSS (and therefore do not need to undergo PA-DSS reviews):

- Operating systems onto which a payment application is installed (for example, Windows, Unix)
- Database systems that store cardholder data (for example, Oracle, PostgreSQL)
- Back-office systems that store cardholder data (for example, for reporting or customer service purposes)

***Note**: The Council has published guidance on applications eligible for PA-DSS, which is available on our website. www.pcisecuritystandards.org/document_library*

PA-DSS Applicability

Type of Payment Application*	Does PA-DSS Apply?
"Off-the-shelf" standard payment applications without much customization	**YES**
Software developed in modules	**YES**, applies to any module with payment functions
For hardware terminals	**YES**, if terminal meets specific criteria
Software developed by application service providers only as a service	**NO**, unless application is sold, licensed, or distributed to third parties
Non-payment application that is part of a payment application suite	**NO**, such applications can be included in a PA-DSS review, bu are not required to be included
Software for only one, typically large, customer, developed to customer's specifications	**NO**, application is covered as part of customer's PCI DSS review
Software developed by merchant or service provider, and used only in-house	**NO**, application is covered as part of merchant's or service provider's PCI DSS review
Supporting systems, for example, operating systems, databases, back-office systems, firewalls, routers, etc.	**NO**, these are not payment applications

*Payment applications are those that store, process, or transmit cardholder data as part of authorization or settlement.

PA-DSS Applicability – Hardware Terminals

There are two ways for a hardware terminal payment application to achieve PA-DSS validation:

1. The payment application directly meets all PA-DSS requirements
2. The payment application is resident on a PCI PTS approved Point of Interaction (POI) hardware device that meets some of the PA-DSS requirements

PA-DSS requirements may be met through a combination of PA-DSS and PTS validated controls:

- Hardware termina must be a PTS validated POI device
- PTS validated hardware provides a trusted computing environment
- Hardware and payment application are required dependencies
- PCI DSS compliant settings must be enabled by default

Knowledge Check

Which of the following could PA-DSS appy to?

- a) Third-party payment application designed for one company
- b) Custom payment applicatin endrsed by the PCI SSC
- c) Custom payment application used by one company
- ✓ d) Third-party, "off-the-shelf" payment application

Next

The QIR Program

- Certification for Qualified Integrators and Resellers (QIRs)
- Assure quality and provide feedback

What is the Role of an Integrator or Reseller?

Integrators and Resellers are those entities that sell, install, and/or service payment applications on behalf of software vendors or others.

Authorized by the software vendor

QIR Responsibilities are likely to include:

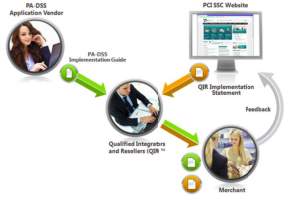
- Implementing the application into the merchant environment
- Integrating the application into other software and systems, where applicable
- Configuring the payment application (where configuration options are provided)
- Servicing the payment applications (for example, troubleshooting, delivering remote updates, and providing remote support)

Why are QIRs so Important to Data Security?

- QIRs have an important role to play in securing account data
- Software vendors are responsible for developing applications
- Applications usually have configuration or installation options which could impact security. For example:
  - Logging of events may be a configurable option
  - The software may have a debug mode for troubleshooting
  - Remote access may be needed to provide support when problems occur

Even though the software vendor may have developed an application which is capable of being secure, the Integrator/Reseller must ensure it is implemented properly and in a secure manner to facilitate PCI DSS compliance.

QIR Documents



Roles and Responsibilities of the Customer

- Organizations using QIR services are encouraged to read and understand the customer's responsibilities under the QIR Customer section of the QIR Program Guide, as well as the QIR Implementation Statement for customer roles and responsibilities. Each merchant and service provider is responsible for their PCI DSS compliance.
- A Qualified Installation does not guarantee PCI DSS compliance but is a good step towards compliance. On its own, a Qualified Installation does not make a merchant or service provider compliant.

QIR Implementations and PCI DSS

How does a Qualified Installation impact the PCI DSS assessment?

- Documentation from a Qualified Installation provides useful information about how the application was installed/configured.
- Application configuration may have changed since the installation.
- Assess the current implementation.
- The assessor's role is not to challenge the Qualified Installation

Knowledge Check

Use of a Qualified Integrator/Reseller (QIR):

a) Is required by PCI DSS

b) Is a good step towards PCI DSS compliance

c) Replaces the need for PCI DSS

d) Ensures PCI DSS compliance

Next

What is a P2PE Solution?

A validated P2PE solution is one that has been verified by a P2PE assessor as meeting all requirements of the P2PE standard, and has been accepted and listed by PCI SSC.

A P2PE solution must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE-validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration, and usage

P2PE and Other PCI Standards

Many of the P2PE requirements are based on elements of other PCI standards:

- POI devices are PCI-approved PIN Transaction Security (PTS) devices
- Requirements for secure cryptographic key operations for both encryption and decryption environments are derived from the PCI PIN Security Standard
- Applications on POI devices meet requirements derived from the Payment Application Data Security Standard (PA-DSS)
- The decryption environment is PCI DSS compliant

Important: *PCI PTS/PIN requirements specify an independent set of control requirements for protection of PIN/PIN block data; the P2PE standard does not supersede or replace any requirements in the PCI PTS/PIN standard.*

Use of P2PE Solutions

Merchants may be able to reduce their PCI DSS scope when using validated, Council-listed P2PE solutions. Merchants using third-party P2PE solutions:

- Merchant environment isolated from clear-text account data.
  - Merchant has no access to account data within encryption device (POI) or decryption environment (at third-party Solution Provider)
- Merchant has no involvement in encryption or decryption operations, or cryptographic key management
  - All cryptographic operations managed by Solution Provider
- Merchant does not have access to security configurations of POI devices or applications
- Merchant isolates any other payment channels from the P2PE environment

Merchants managing their own P2PE solutions:

- P2PE version 2.0 provides options for merchants managing their own P2PE solution

P2PE Overview

P2PE does not replace PCI DSS.

Use of a PCI P2PE Solution can help to reduce PCI DSS scope.

- Must use a validated and listed PCI P2PE solution.
- Validated P2PE solutions, POIs, and other P2PE solution information listed on the PCI SSC website.

Merchants should consult with their acquirer or the payment brands about using encryption solutions not included on PCI SSC's list of validated P2PE Solutions.

Knowledge Check

The presumption of P2PE is that:

✓ a) The data cannot be decrypted between the source and the destination points

b) Any entity in possession of the ciphertext can easily reverse the encryption process

c) The data can be decrypted between the source and the destination points

d) The data can never be decrypted

Next

Knowledge Check

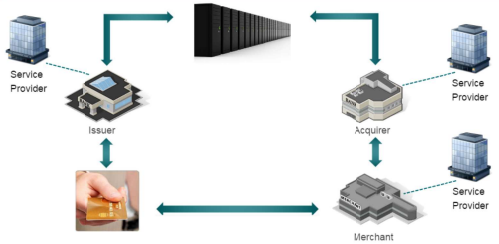
Merchants using P2PE solutions are still required to validate to PCI DSS.

✓ True

False

Next

Compliance Within the Payment Process



Roles & Responsibilities: PCI Security Standards Council

Role of the Council

- Maintain PCI DSS, PA-DSS, PTS, P2PE, Card Production, and PIN Security standards and supporting documentation
- Define and Implement Qualification Requirements for QSAs, PA-QSAs, ASVs, and ISAs
- Approve companies and their employees to perform PCI DSS assessments, Payment Application assessments, and ASV scanning
- Post list of QSA, PA-QSA, and ASV companies on Website
- Maintain list of validated payment applications
- Maintain list of approved PIN Transaction Security (PTS) devices
- Maintain list of validated P2PE solutions
- Review selected reports (ROCs, ROVs, P-ROVs and ASV scan reports) for quality assurance
- Offer training for the QSAs, PA-QSAs, ASVs, ISAs, QIRs, and PCIPs
- Offer general PCI Awareness training to the community
- Offer additional guidance on specific technologies as needed
- Promote payment card security on a global basis

PCI Security Standards Council

Roles & Responsibilities: Payment Brands

Payment Brands – the members of PCI SSC (American Express, Discover, JCB, MasterCard, Visa) are responsible for:

- Development and enforcement of compliance programs
- Fines or penalties for non-compliance
- Endorse QSA, PA-QSA, and ASV company qualification criteria
- Accept validation documentation from approved QSA, PA-QSA, and ASV companies and their employees
- Provide feedback to the Council on QSA, PA-QSA, and ASV performance
- Forensic investigations of account data compromise

AMERICAN EXPRESS DISCOVER JCB MasterCard VISA

Roles & Responsibilities: Qualified Security Assessor

- Validate the scope of the assessment
- Conduct PCI Data Security Standard assessments
- Verify all technical information given by merchant or service provider
- Use independent judgement to confirm PCI DSS requirements have been met
- Be onsite for the duration of any relevant assessment procedure
- Review the work product that supports the assessment procedures
- Adhere to the PCI DSS Requirements and Security Assessment Procedures
- Select representative samples of business facilities and system components where sampling is employed
- Evaluate compensating controls
- Produce the final Report on Compliance

Roles & Responsibilities: Internal Security Assessor

- Validate scope of the assessment
- Conduct PCI Data Security Standard assessments
- Verify all technical information given by stakeholders
- Use independent judgement to confirm requirements have been met
- Provide support and guidance during the compliance process
- Be onsite for the duration of any relevant assessment procedure
- Review the work product that supports the assessment procedures
- Adhere to the PCI DSS Requirements and Security Assessment Procedures
- Select representative samples of business facilities and system components where sampling is employed
- Evaluate compensating controls
- Produce final report

Roles & Responsibilities: Approved Scanning Vendor

- Performing external vulnerability scans in accordance with PCI DSS Requirement 11.2, and other supplemental guidance published by the PCI SSC
- Making reasonable efforts to ensure scans:
  - Do not impact the normal operation of the scan customer environment
  - Do not penetrate or intentionally alter the customer environment
- Scanning all IP ranges and domains provided by scan customer to identify active IP addresses and services
- Consulting with the scan customer to determine if IP addresses found, but not provided by the scan customer, should be included
- Providing a determination as to whether the scan customer's components have passed the scanning requirements
- Providing adequate documentation to demonstrate the compliance or non-compliance of the scan customer's components

Roles & Responsibilities: Merchants & Service Providers

- Review and understand the PCI Security Standards
- Understand the compliance validation and reporting requirements defined by the payment card brands
- Validate and report compliance to acquirer or payment card brand as applicable
- Maintain ongoing compliance, not just during assessment
- Read and incorporate communications from the payment brands, acquirers, and the PCI SSC throughout the year

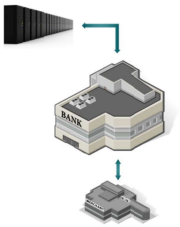
Roles and Responsibilities: PA-QSA

The Payment Application Qualified Security Assessor (PA-QSA) has the following responsibilities:

- Performing payment application assessments per the PA-DSS and the PA-QSA Validation Requirements
- Providing opinions regarding payment applications' compliance with PA-DSS requirements
- Providing adequate documentation within ROV to show that payment application is PA-DSS compliant
- Submitting the ROV to PCI SSC, along with the Attestation of Validation
  - Signed by both PA-QSA and vendor
- Maintaining an internal PA-QSA quality assurance process

Roles and Responsibilities: Acquirer

- Compliance validation for their merchants
  - When and how to report
- Determine merchant levels and reporting process
- Accept merchant compensating controls
- Procedures for cata breaches at their merchants
  - Reporting to payment brands
  - Supporting forensic investigations
  - Understanding other payment brand responsibilities after breach at merchants
- Familiar with each payment brand's compliance validation programs



Knowledge Check

Which entity is responsible for developing and enforcing compliance programs?

- a) Issuers
- b) PCI SSC
- ✓ c) Payment card brands
- d) Acquirers

Next

Roles and Responsibilities: QIR

- Install payment applications in a manner which supports the customer's PCI DSS compliance
- Provide customers with a completed Implementation Statement after installation
- Document for the customer any potential risks to PCI DSS compliance
- Provide a Feedback Form to the customer

Knowledge Check

Which entity is responsible for forensic investigations of account data compromise?

- a) PCI SSC
- ✓ b) Payment Brands
- c) QSA/ISA
- d) QIR

Next

Module Summary

In this module, we have discussed:

- Payment Brand Compliance Programs
- SAQ Overview
- PA-DSS Overview
- Qualified Integrator/Reseller (QIR) Overview
- P2PE Overview
- PCI Roles and Responsibilities

Roles and Responsibilities – QSA

- Adhere to the QSA Qualification Requirements
- Read and incorporate communications from the payment brands and PCI SSC throughout the year
- Conduct follow-up assessments if required
- Send any administrative or technical questions to your company's primary contact person
- Help your company maintain ongoing compliance

Module Overview and Objectives

Module Topics:

- Additional QSA Responsibilities
- QSA Qualification Requirements
- Code of Professional Responsibility
- PCI SSC Assessor Quality Management (AQM) Program

Module Objectives:

After completing this module, you will be able to:

- Describe the additional responsibilities of a QSA.
- Outline the Qualification Requirements in the context of the following:
  - Adherence to PCI procedures
  - Evidence retention
  - QSA qualification requirement
- Define the guiding principles of the Assessor Quality Management Program
- Understand the PCI SSC Code of Professional Responsibility

Keeping Up To Date

Keeping up to date includes reviewing:

- New and updated FAQs
- New Information Supplements
- Monthly Assessor Newsletters
- Program and Standards updates

Visit the PCI SSC Website for new and updated information

QSA Qualification Requirements

The current version of the PCI DSS Qualification Requirements for Qualified Security Assessors describes the necessary qualifications a QSA must have to be recognized by the PCI SSC to perform assessments.

QSA Independence Requirements

- The QSA must adhere to professional and business ethics, perform all duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing Assessments
- The QSA will not undertake to perform Assessments of entities that it controls or with which it is under common control or in which it holds any investment
- The QSA must fully disclose in the Report on Compliance if they assess customers who use any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights, or that the QSA has configured or manages
- The QSA agrees that when the QSA recommends remediation actions that include one of its own solutions or products, the QSA will also recommend other market options that exist

Adherence to PCI Procedures

- The QSA report must follow the Report on Compliance (ROC) template and instructions, or the applicable SAQ
- The QSA must prepare each report based on evidence obtained by following the PCI DSS Requirements and Security Assessment Procedures (PCI DSS)
- The QSA must accompany a ROC with an "Attestation of Compliance", signed by the QSA and any related findings

QSA Quality Assurance Requirements

- The QSA must have implemented a quality assurance program as documented in their quality assurance program manual
- The QSA must provide a QSA Feedback Form to their client at the start of the assessment
- The QSA must adhere to all quality assurance requirements mandated by PCI SSC
- PCI SSC reserves the right to conduct site-visits and audit the QSA at the discretion of the PCI SSC
- Upon request, the QSA must provide their quality assurance manual to PCI SSC

Protection of Confidential and Sensitive Informatıcn

- The QSA must maintain adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect sensitive and confidential information against any threats or unauthorized access during storage, processing, and/or communicating of this information
- The QSA must maintain the privacy and confidentiality of information obtained in the course of performing their duties under the QSA Agreement, unless (and to the extent) disclosure is required by legal authority

Maintaining QSA Qualification

- Pay annual re-qualification fees
- Complete PCI SSC training (Instructor Led Training Initially – On-Line CBT for Subsequent Years) on an annual basis
- Provide proof of security training within last 12 months
- 20 CPE hours per year / 120 CPE hours over 3 years
- Receive satisfactory evaluations from clients and payment card brands

Evidence Retention

- The QSA must secure and maintain digital and/or hard copies of case logs, audit results and work papers, notes, and any technical information that was created and/or obtained during the PCI Data Security Assessment for a minimum of three (3) years
- The QSA must provide a copy of the evidence retention policy and procedures to PCI SSC upon request

QSA Revocation Process

A QSA (or any QSA employee thereof) may have their qualification revoked if found to be in breach of the Agreement, including the following:

- The QSA fails to validate compliance in accordance with the PCI DSS Requirements and Security Assessment Procedures and/or the PA-DSS Requirements and Security Assessment Procedures, as applicable
- The QSA violates any provision regarding non-disclosure of confidential materials
- The QSA fails to maintain physical, electronic and procedural safeguards to protect the confidential and sensitive information and/or fails to report unauthorized access to systems that are storing confidential and sensitive information
- The QSA engages in unprofessional or unethical business conduct
- The QSA (or any QSA employee thereof) is determined to have cheated on any exam in connection with QSA, PA-QSA, or any other PCI SSC sanctioned training

Knowledge Check

QSAs must secure and maintain digital and/or hard copies of case logs, audit results and work papers, notes, and any technical information what was created and/or obtained during the assessment for a minimum of _____.

- a) 5
- ✓ b) 3
- c) 1
- d) 2

Next

Knowledge Check

The QSA Qualification Requirements document: (choose all that apply)

- a) Includes a template for completing the ROC
- ✓ b) Is available on the PCI SSC website
- ✓ c) Is required reading for QSAs
- ✓ d) Describes the necessary qualifications a QSA must have to maintain their qualification

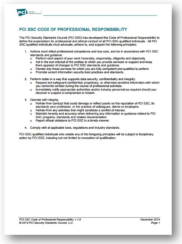
Next

Principles

Code of Professional Responsibility Principles:

- Actions must reflect professional competence and due care, and be in accordance with PCI SSC standards and guidance
- Perform duties in a way that supports data security, confidentiality and integrity
- Operate with integrity
- Complying with all applicable laws, regulations, and industry standards

Download the Code from the PCI SSC Document Library

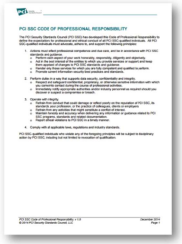


Adherence to the Code

All PCI SSC-qualified individuals are required to advocate, adhere to, and support these principles.

PCI SSC-qualified individuals who violate the principles will be subject to disciplinary action by PCI SSC, including but not limited to revocation of qualification.

Download the Code from the PCI SSC Document Library



AQM Program Objective

The current version of the PCI DSS Qualification Requirements for Qualified Security Assessors describes the necessary qualifications a QSA must have to be recognized by the PCI SSC to perform assessments.

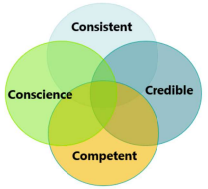
Guiding Principles Validated by Four Criteria

Consistent
- Limited deviation of Assessment

Credible
- Opinions stated are valid, exhaustive, and defendable

Competent
- Appropriate level of understanding

Conscience
- Work performed in association with a PCI SSC program is ethical and adheres to requirements



Guiding Principles

Principle 1: Best interest of assessor client is upheld

Principle 2: Assessor company adheres to Qualification Requirements

Principle 3: Assessor employee adheres to Qualification Requirements

Principle 4: Assessor procedures and reporting are consistent

Principle 5: Assessor appropriately interprets the PCI Standards as applicable to their client's systems and environment

Principle 6: Assessor stays current with industry trends and PCI SSC updates

Principle 7: All opinons rendered are factual, documented, and defendable

Principle 8: Assessor maintains a positive relationship with PCI SSC

AQM Assurance Tiers

Qualifying Assessor Companies by ensuring appropriate levels of capability and experience as defned in each program's Qualification Requirements

Qualifying Assessor Employees through resume reviews, face-to-face training sessions and CBTs, and qualification exams

Security Assessment Report Reviews o provide reasonable assurance that security products are within the scope of the applicable program, meet all of that program's requirements, and support a merchant's overall DSS compliance

Assessor Company Audits that review detailed quality of work product and acherence to internal quality processes

AQM Assurance Tiers by PCI Program

AQM activities include:

Assurance Tier	PCI DSS			PA-DSS	P2PE	PFI	PTS
	QSA	ISA	ASV	PA-QSA	QSA (P2PE) PA-QSA (P2PE)	PFI	PTS Labs
Qualifying Companies	✓		✓	✓	✓	✓	✓
Qualifying Employees	✓	✓	✓	✓	✓	✓	
Review reports, submissions for SSC listings				✓	✓		✓
Company Audit	✓		✓	✓	✓	✓	✓

Report Reviews

- Product-focused programs (PA-DSS, PTS) and solution-focused programs (P2PE) require that validation reports be submitted to PCI SSC for review
- Goals of these reviews are to determine:
  - Is the security product within the scope of the applicable program
  - Is the report complete and does it evidence that all test procedures have been completed by the assessor in detail consistent with the Reporting Instructions
- If accepted, submitted products are listed on the PCI SSC website
- AQM team will identify any persistent quality issues in reporting

Qualifying Assessors

A set of Qualification Requirements exist for all PCI SSC Assessor programs that:

- Set the minimum acceptable requirement to become an assessor company/employee
- Include Terms and Conditions that govern the operations of each program

Assessor Companies

- Internal quality assurance program
- Corporate experience, facility expectations, independence, insurance
- Minimum number of employee & required roles

Assessor Employees

- Pre-requisite education, training, certifications
- PCI training requirements

Assessor Company Audits

Outcomes of audits can include the following:

Report Review & Audit Outcomes	Action
Satisfactory	Notification Letter with specific opportunities for improvement listed; Call with the AQM team to discuss
Needs Improvement	Warning Letter with specific opportunities for improvement and other improvement activities; Mandatory call with the AQM team to discuss
Unsatisfactory	Unsatisfactory Letter with specific opportunities for improvement listed; Mandatory call with the AQM team to discuss Remediation

Criteria for audit outcomes vary for each PCI program.

Remediation

- Remediation Overview Call and signed Remediation Agreement
- Remediation Period is at least 90 days
- Assessor website listing updated to "Red" to notify merchants/service providers
- The assessor company will have a case manager assigned to them who will offer support to the assessor company as their work to bring their quality level to the expected baseline standard of quality
- The AQM team will provide increased support and guidance during the Remediation Period
- Successful completion requires strong commitment from the assessor company
- Fees will be charged to review work

Types of Violations

Severity Level	Examples
Critical Violation	Intentionally hiding that a client stores track data, failure to renew insurance, non-assessor employee leading a PCI engagement, intentional misrepresentation of Standards, documenting non-compliant controls as "in place"
Standard Violation	Requiring additional procedures beyond the testing procedures, failing to appropriately document all validation procedures, compensating contros worksheet incomplete
Administrative Violation	Assessor employee does not attend training but continues to lead engagements, Non-disclosure of services reviewed that are performed or managed by the same organization, failure to have SSC approve sub-contractor
Information Violation	Failure to document CPE credit, failure to respond to SSC request in a timely manner

Revocation

- PCI Council will evaluate issue as well as any associated appeal
- Assessor or assessor employee will be removed from assessor list
- At a minimum, assessor will not be allowed to reapply for 180 days
- If the assessor reapplies, there must be evidence of an improved internal QA program and other requirements

Stages for Violations

Identify

- PCI SSC will determine whether the violation is that of the assessor company, assessor employee, or both
- Historical review of previous violations as well as feedback will be considered

Notify

- Warning letter issued to assessor company and assessor employees involved in the incident, unless immediately escalated

Escalate

- Escalated case will be presented to the SSC to determine action including remediation or revocation

Knowledge Check

An example of a "Crtical Violation" of the AQM program is:

- a) Documenting non-compliant controls as "In Place"
- b) Not submitting reports periodically
- c) Refusal to submit a ROC/AOC for a non-compliant merchant
- d) Failing to document CPEs

Next

Module Overview and Objectives

Module Topics:

- Cardholder Data Discovery
- Network Segmentation
- Scoping the Cardholder Data Environment

Module Objectives:

After completing this module, you will be able to:

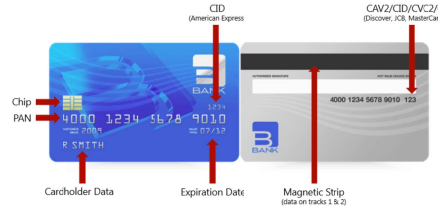
- Explain common storage scenarios for cardholder data and sensitive authentication data
- Outline processes for cardholder data discovery
- Define network segmentation
- Understand the impact of network segmentation on scoping for PCI DSS
- Identify forms of network segmentation
- Explain how to scope a PCI DSS assessment
- Identify common errors in PCI DSS scoping

Module Summary

In this module, we discussed:

- Additional QSA Responsibilities
- QSA Qualification Requirements
- Code of Professional Responsibility
- PCI SSC Assessor Quality Management (AQM) Program

Types of Data on a Payment Card



Cardholder, Track, and Sensitive Authentication Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full magnetic stripe data (or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

PCI DSS applies wherever account data is stored, processed, or transmitted. Account data consists of cardholder data and/or sensitive authentication data, as follows:

- Many people refer to ALL account data simply as "Cardholder Data"
- PCI DSS requirements are applicable wherever Primary Account Number (PAN; or Sensitive Authentication Data (SAD) is stored, processed, or transmitted
- PCI DSS requirements also apply to systems that provide security services or could impact the security of account data
- Account data includes all of the information printed on the physical card as well as the data on the magnetic stripe or chip
- Sensitive Authentication Data cannot be stored after authorization
- Encrypting cardholder data or sensitive authentication Data does NOT necessarily remove it from scope

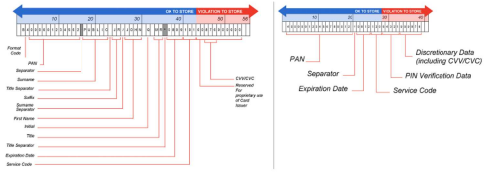
PCI DSS and Chip Transactions

- Merchants are not permitted to store the track equivalent data following authorization
- Track equivalent data found on the chip differs from the track data found on the magnetic stripe, as the chip track data contains a unique Chip CVV/CVC code
- This prevents criminals from producing cloned magnetic stripe cards from chip track data
- However there is still sufficient information to allow criminals to use this data in card-not-present fraud (such as e-commerce or mail order/telephone order)

Track 1 vs. Track 2 Data

Payment cards typically use two tracks of payment data on the magnetic stripe:

- Track 1
  - Contains all fields of both Track 1 and Track 2
  - Length up to 79 characters
- Track 2
  - Provides shorter processing time for older dial-up transmissions
  - Length up to 40 characters



Where Does Cardholder Data Flow?

- Cardholder data flows between and through applications, systems, and network infrastructure devices
- It is very important to document all cardholder data flows prior to beginning any assessment activities
- An inventory of some kind should be developed to identify all systems that store, process, or transmit cardholder data

An Inventory

An inventory of all systems that store, process, and/or transmit cardholder data must be maintained.

The inventory may be in any usable format.

Suggestion: Information to be maintained in the inventory could include:

- System name
- Cardholder data stored (list fields)
- Reason for storage
- Retention period
- Protection mechanism
  - Including methods for protecting stored PANs per PCI DSS 3.4 (hashing, encryption, or truncation)

System Name	Account Data Stored	Reason for Storage	Retention Period	Protection Mechanism

Storing Track Data is Not Permitted

It is not permitted to store full track data or other sensitive authentication data after authorization This applies even if the data is protected by:

- Encryption
- Password protection
- Data scrambling/obfuscation
- Masking
- Proprietary data formats
- Other mechanisms

Exceptions:

- Issuers and issuing processors may be permitted to retain sensitive authentication data if needed for business purposes
- Payment brands may have additional requirements for issuers

Where is Cardholder Data Stored?

- Cardholder data is stored in both known and unknown locations on most networks.
- Cardholder data can "leak" out of known storage locatons.
- Having a good inventory could be the starting point to identify cardholder data storage locatons.
- Entities may need to perform a thorough search of all systems to identify cardholder and track data.

Storing Track Data For Troubleshooting Purposes

Businesses may have a need to store track data (temporarily) for troubleshooting purposes

- Why? Track misreads, network errors, encryption issues, etc.

Ensure documented procedures include:

- Collecting sensitive authentication data only when needed to solve a specific problem
- Collecting the minimum amount of data needed to solve the specific problem
- Storing any such data in a specific, secure location with limited access
- Do not retain more data than needed
- Encrypt data when stored/transmitted
- Securely delete data immediately when troubleshooting is complete
- Include a destruction practice
- Verify data cannot be retrieved once troubleshooting is complete

Track Data Location

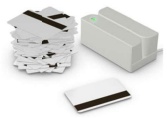
Track data can be found in a variety of data stores:

Typical location of track data storage include:

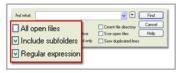
- Databases
- Flat files
- Log files
- Debug files

Systems that commonly store track data:

- POS systems
- POS servers
- Authorization servers



General Guidelines For Searching



Regular Expression Searching

- Makes the job easier
- Supported by many freeware and commercial tools

Validation

- Regular expressions may produce false positives
- Validate as many elements as you can:
  - MOD-10, the account number
  - Validate total track length

CAV2/CID/CVC2/CVV2 Data Location

Card verification value or code (CAV2/CID/CVC2/CVV2) data can be found in a variety of data stores.

Typical location of card verification value or codes include:

- Paper
- Databases
- Flat files
- Log files
- Debug files

Systems that commonly store card verification value or code data:

- Authorization servers
- Web servers
- Kiosk

Card verification value or codes are NOT required for recurring card-not-present transactions.

MOD-10 (The Luhn Formula)

If you find a potential card number, you can use a MOD 10 check to see if it is a valid card number.

Step 1: Double the value of alternate digits of the primary account number beginning with the second digit from the right. For any resulting value >=10, subtract 9.
Step 2: Add the calculated values as well as the values skipped in Step 1 together.
Step 3: The total obtained in Step 2 must be divisible by 10.

4	4	0	8	9	8	5	5	1	0	0	0	0	5	8	5
x2		x2		x2		x2		x2		x2		x2		x2	
8		0		18		10		1		0		0		16	
				-9		-9								-9	
8	4	0	8	9	8	1	5	1	0	0	0	0	5	7	5

Cardholder Data Discovery Tools

Vast array of tools available for data discovery

- Commercial products
- Freeware and/or open source software
- Forensics tools
- Data Loss Prevention
- Proprietary

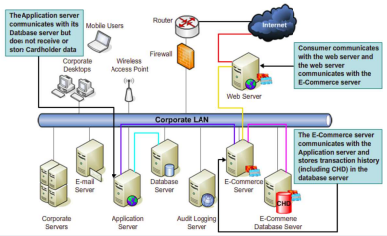
Check with your IT, security, or audit departments.

What works well in one organization may not be the best choice in another organization.

**Use of data discovery tools is not a requirement.*

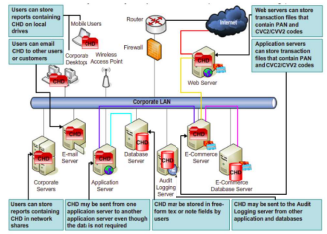
Cardholder Data Discovery Case Study 1

Cardholder Data Flow Example



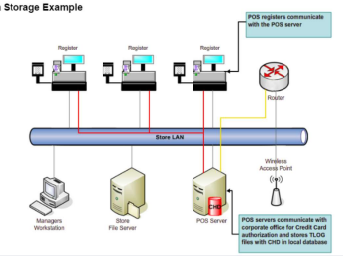
Cardholder Data Discovery Case Study 2

Cardholder Data Storage Example



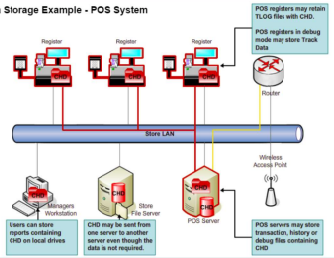
Cardholder Data Discovery Case Study 3

Cardholder Data Storage Example



Cardholder Data Discovery Case Study 4

Cardholder Data Storage Example - POS System



Knowledge Check

Storing track data is permitted when _____.

- a) it is encrypted by the merchant storing it
- b) it is hashed by the merchant storing it
- c) it is reported to the PCI SSC annually in a ROC
- ✓ d) it is being stored by issuers with a business justification

Next

Knowledge Check

Account data consists of _____ and _____ ?

- ✓ a) Cardholder Data, Sensitive Authentication Data
- b) PANs, PINs
- c) Cardholder Names, PANs
- d) Cardholder Data, PANs

Next

Knowledge Check

When scoping an environment for PCI DSS, it is important to identify _____.

(select all that apply)

- ✓ a) Business facilities involved in processing transactions
- ✓ b) Personnel with access to cardholder data
- ✓ c) All flows of cardholder data
- ✓ d) Components that store cardholder data

Next

Knowledge Check

Which of these devices can be used to provide network segmentation controls?
(select all that apply)

- [x] a) Firewalls
- [ ] b) File servers
- [x] c) Switches
- [x] d) Routers

Next

Scope of PCI DSS

- PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment
- The cardholder data environment is comprised of people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data
- "System components" include network devices, servers, computing devices, and applications

Network Segmentation Overview

- Scope of PCI DSS
- Network Segmentation
- What are acceptable forms of Network Segmentation?
- Network Segmentation Case Study

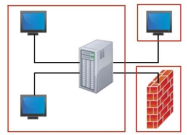
Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement.

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.

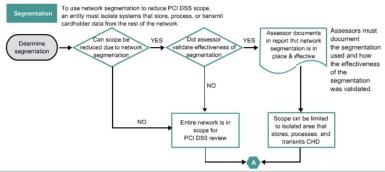
Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technology that restricts access to a particular segment of a network.

Any device that isolates the cardholder data environment from the rest of the network could be used for segmentation.

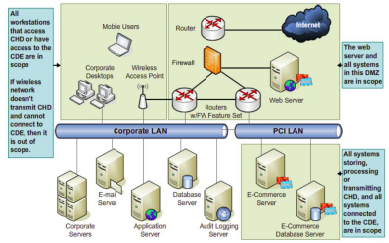


What are Acceptable Forms of Network Segmentation?

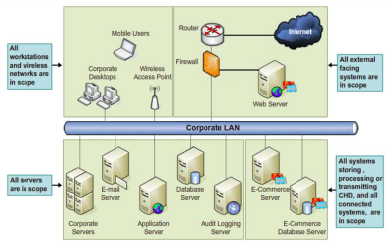
- At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not
- To be out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE
- If network segmentation is being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate
- The implementation of network segmentation is highly variable and dependent upon a number of factors



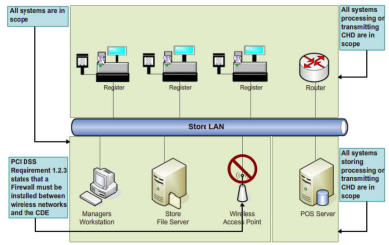
Network Segmentation Case Study (With Segmentation)



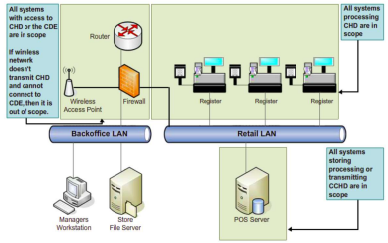
Network Segmentation Case Study (No Segmentation)



Network Segmentation Case Study (No Segmentation)



Network Segmentation Case Study (With Segmentation)



How to Scope a PCI DSS Assessment

PCI DSS requirements apply to all system components included in or connected to the cardholder data environment.

The cardholder data environment (CDE) comprises people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.

Examples of system components that may be in scope include, but are not limited to:

- Systems providing security services, segmentation, or that impact the security of the CDE
- Virtualization components
- Network components such as firewalls, switches, routers, wireless access points, network appliances, and other security appliances
- Servers such as Web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name system (DNS)
- Applications including internal and external (for example, Internet) applications
- Any other component or device located within or connected to the CDE

How to Scope a PCI DSS Assessment

- How many applications store, process or transmit cardholder data?
- How many databases support the in-scope applications?
- List all database platforms that store credit card data (Oracle, MS SQL, DB2)?
- How many servers store, process or transmit cardholder data to support the applications in scope?
- What are the operating systems for the servers (MS, UNIX, Linux, AS400, etc.)?
- Is there segmentation between the systems storing credit card data and the rest of the network?
- How many Internet, DMZ, or segmentation firewalls are in place?
- How is the segmentation achieved (VLAN, Firewall, etc.)?
- Is wireless technology in use anywhere on the network? If so, how many locations?
- Is credit card data transmitted over wireless devices at any point?
- Are credit card transactions accepted through a web server?
- Are credit card numbers stored on the POS systems for any length of time?
- How many data centers store, process or transmit cardholder data?
- How many call centers store, process or transmit cardholder data?
- Is any part of the environment outsourced?
- Are there third parties, outsourcers, or business partners connected to the network?

- The assessor should have a thorough understanding of the environment being assessed, including the system components and physical locations where cardholder data is stored, processed, or transmitted.
- Data flow diagrams help identify where cardholder data could exist.
- An inventory should be completed to document all in-scope systems.
- An adequate amount of time should be allowed to complete a thorough assessment of the cardholder data environment.

Common Errors in PCI DSS Scoping

- Not having a complete inventory of all systems that store, process, or transmit cardholder data
- Not identifying "unknown" data that has "leaked" out of applications and databases
- Not identifying all physical locations that store, process or transmit cardholder data
- Not identifying all connected networks and confirming network segmentation is in place and effective
- Not allowing enough time to interview all application, database, and system owners
- Not allowing enough time to perform thorough system testing
- Assuming encrypted data is out of scope

Reducing the Scope of a PCI DSS Assessment

The fastest way to reduce the scope of the PCI DSS Assessment is to not store cardholder data

If cardholder data is stored, consider other forms of meeting requirement 3.4 than encryption:

- Removal of cardholder data
- Truncation and one-way hashes based on strong cryptography are alternatives to encryption

***Note**: Systems that receive PAN before it is truncated/hashed, or that perform or are connected to the systems that perform the truncation or hashing, are always in scope.*

PCI DSS Assessment Sampling

After considering the overall scope and complexity of the environment being assessed, the assessor may select representative samples of business facilities and system components in order to assess PCI DSS requirements.

Principles of sampling include:

- Consideration for business facilities and system components.
- Samples must be a representative selection of all types and locations of business facilities, as well as all types of system components.
- Samples must be sufficiently large enough to provide the assessor with assurance that controls are implemented as expected.

Examples of business facilities may include:

- Corporate offices
- Datacenters
- Call centers
- Retail stores
- Franchise merchants

Knowledge Check

If virtualization technologies are used in a cardholder data environment:

- a) The virtualization technologies are not in scope for PCI DSS
- b) Entities using virtualization technologies should complete SAQ C
- c) Virtualization technologies should not be used in the cardholder data environment
- ✓ d) The virtualization technologies are included in scope for PCI DSS

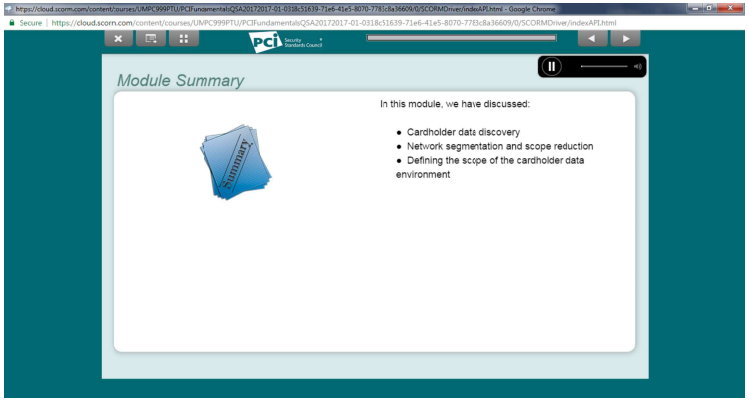
Next

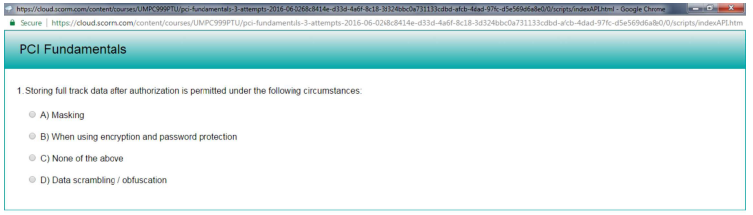
Knowledge Check

Entities involved in payment card processing via mobile devices (like a phone or tablet) can reduce the risks to the security of cardholder data by:

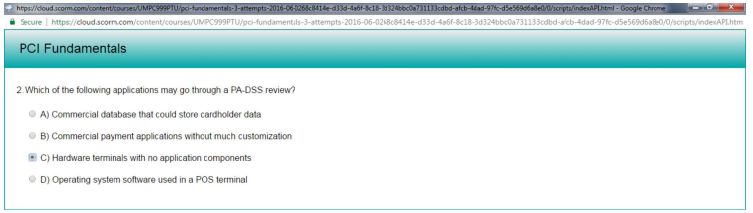
- a) Encrypting account data within the mobile device using an approved encryption application
- ✓ b) Encrypting account data at the point of capture using an appoved point of interaction device
- c) Inputting account data directly into the mobile device
- d) Storing account data within the motile device

Next


Secure | https://cloud.scorm.com/content/courses/UMPC999PTU/PCIFundamentalsQSA20172017-01-0318c51639-71e6-41e5-8070-77E3c8a36609/0/SCORMDriver/indexAPI.html
Module Summary
In this module, we have discussed:
Cardholder data discovery
Network segmentation and scope reduction
Defining the scope of the cardholder data environment
Summary


Secure | https://cloud.scorm.com/content/courses/UMPC999PTU/pci-fundamentals-3-attempts-2016-06-0248c8414e-d33d-4a6f-8c18-3d324bbc0a731133cdbd-afcb-4dad-97fc-d5e569d6a8b0/0/scripts/indexAPI.htm
PCI Fundamentals
1. Storing full track data after authorization is permitted under the following circumstances:
A) Masking
B) When using encryption and password protection
C) None of the above
D) Data scrambling / obfuscation


01:29:44


Secure | https://cloud.scorm.com/content/courses/UMPC999PTU/pci-fundamentals-3-attempts-2016-06-0248c8414e-d33d-4a6f-8c18-3d324bbc0a731133cdbd-afcb-4dad-97fc-d5e569d6a8b0/0/scripts/indexAPI.htm
PCI Fundamentals
2. Which of the following applications may go through a PA-DSS review?
A) Commercial database that could store cardholder data
B) Commercial payment applications withcut much customization
C) Hardware terminals with no application components
D) Operating system software used in a POS terminal


01:23:51
Submit and Continue