

Session 2: Self Assessment Questionnaire and Network Scans

Kurt Hagerman

CISSP, QSA

Director of IT Governance
and Compliance Services



Agenda

- Session 1: An Overview of the Payment Card Industry
- **Session 2: Self Assessment Questionnaire and PCI Scans**
- Session 3: Application Security
- Q & A

Your Requirements (Level 2,3,4)

If you STORE, PROCESS, or TRANSMIT cardholder data then:

1. You must meet the requirements of the PCI DSS
2. You must fill out a Self Assessment Questionnaire annually
3. You must have quarterly external network scans conducted by a qualified ASV.

What is the Data Security Standard (DSS)

What is the Data Security Standard (DSS)?

- 200+ Specific requirements rather than vague guidelines
- DSS applies to all merchants all major brands.
- Permits for “compensating controls” (a term often misunderstood)
- Includes technical configuration requirements, business justification, policies, risk assessments, etc.
- NOT JUST AN I.T. ISSUE! – Finance, HR, Operations, Legal, etc.

6 Control Objectives, 12 Requirements

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

Sample Requirements

- 1.1 Establish firewall and router configuration standards that include the following:**
 - 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations**
 - 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks**
 - 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone**
 - 1.1.4 Description of groups, roles, and responsibilities for logical management of network components**
 - 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure**
 - 1.1.6 Requirement to review firewall and router rule sets at least every six months**

PCI DSS Security Audit Procedures

PCI DSS REQUIREMENTS	TESTING PROCEDURES
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners)
12.1.1 Addresses all requirements in this specification	12.1.1 Verify that the policy addresses all requirements in this specification.

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and

10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required

Navigating the DSS



Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS

Understanding the Intent of the Requirements

Version 1.1
February 2008

Requirement	Guidance
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following: <ul style="list-style-type: none">12.1.1 Addresses all requirements in this specification12.1.2 Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment12.1.3 Includes a review at least once a year and updates when the environment changes.	<p>A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.</p> <p>Security threats and protection methods evolve rapidly throughout the year. Without updating the security policy to reflect these changes, new protection measures to fight against these threats will not exist.</p>

Quick Review

- The Data Security Standard (DSS) applies to everyone who stores, processes, or transmits cardholder data.
- The DSS has:
 - 6 Control Areas
 - 12 General Requirements
 - 200+ Specific Requirements
- The PCI Assessment Procedures is used by QSA's for formal assessments, and provide testing criteria.
- Navigating the DSS is a document to help merchants with understanding the requirements.



What is the Self Assessment Questionnaire (SAQ)?

Your Requirements (Level 2,3,4)

What you **must do**, and how you **must validate** are totally separate.

All merchants **must be** PCI compliant

Level 2, 3, and 4 merchants **validate** compliance through the SAQ and quarterly scans.

Level	Visa
1	<ul style="list-style-type: none">• Onsite Review by a QSA.• Quarterly Network Scan by ASV.
2	<ul style="list-style-type: none">• Annual Self-Assessment Questionnaire• Quarterly Network Scan by ASV.
3	<ul style="list-style-type: none">• Annual Self-Assessment Questionnaire• Quarterly Network Scan by ASV.
4	<ul style="list-style-type: none">• Annual Self-Assessment Questionnaire• Quarterly Network Scan by ASV.

SAQ and ASA

- SAQ: Self Assessment Questionnaire / ASA: Annual Self Assessment

Available at www.pcisecuritystandards.org

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

SAQ

Self-Assessment Questionnaire (SAQ) Frequently Asked Questions

1. *What is the PCI DSS Self-Assessment Questionnaire?*

The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are four versions of the PCI DSS SAQ to choose from to meet your business need. .

See “Selecting the SAQ and Attestation that Best Apply to Your Organization” in the *Self-Assessment Questionnaire Instructions and Guidelines*.

https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf

SAQ “D”

PCI DSS Compliance - Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ D) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete a clean vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.
3. Complete the Attestation of Compliance in its entirety.
4. Submit the SAQ, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to your acquirer (for merchants) or to the payment brand or other requester (for service providers).

Sample Questions

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Question		Response:	<u>Yes</u>	<u>No</u>	<u>Special*</u>
3.1	(a) Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and/or regulatory purposes?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Compliance/Non-Compliance

Part 3a. Confirmation of Compliant Status

Merchant confirms:

- | | |
|--------------------------|--|
| <input type="checkbox"/> | PCI DSS Self-Assessment Questionnaire D, Version <i>(version of SAQ)</i> , was completed according to the instructions therein. |
| <input type="checkbox"/> | All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects. |
| <input type="checkbox"/> | I have confirmed with my POS vendor that my POS system does not store sensitive authentication data after authorization. |
| <input type="checkbox"/> | I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times. |
| <input type="checkbox"/> | No evidence of magnetic stripe (i.e., track) data ² , CAV2, CVC2, CID, or CVV2 data ³ , or PIN data ⁴ storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment. |

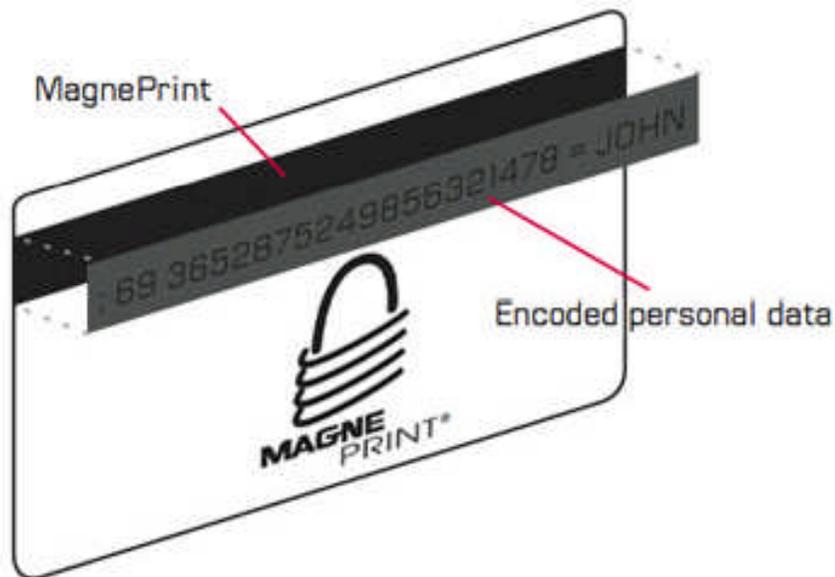


The following slides are VERY important

This is VERY important:

	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number	Yes	Yes
	Cardholder Name ¹	Yes	Yes ¹
	Service Code ¹	Yes	Yes ¹
	Expiration Date ¹	Yes	Yes ¹
Sensitive Authentication Data ²	Full Magnetic Stripe ¹	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/PIN Block	No	N/A

Don't *EVER* keep *TRACK DATA*

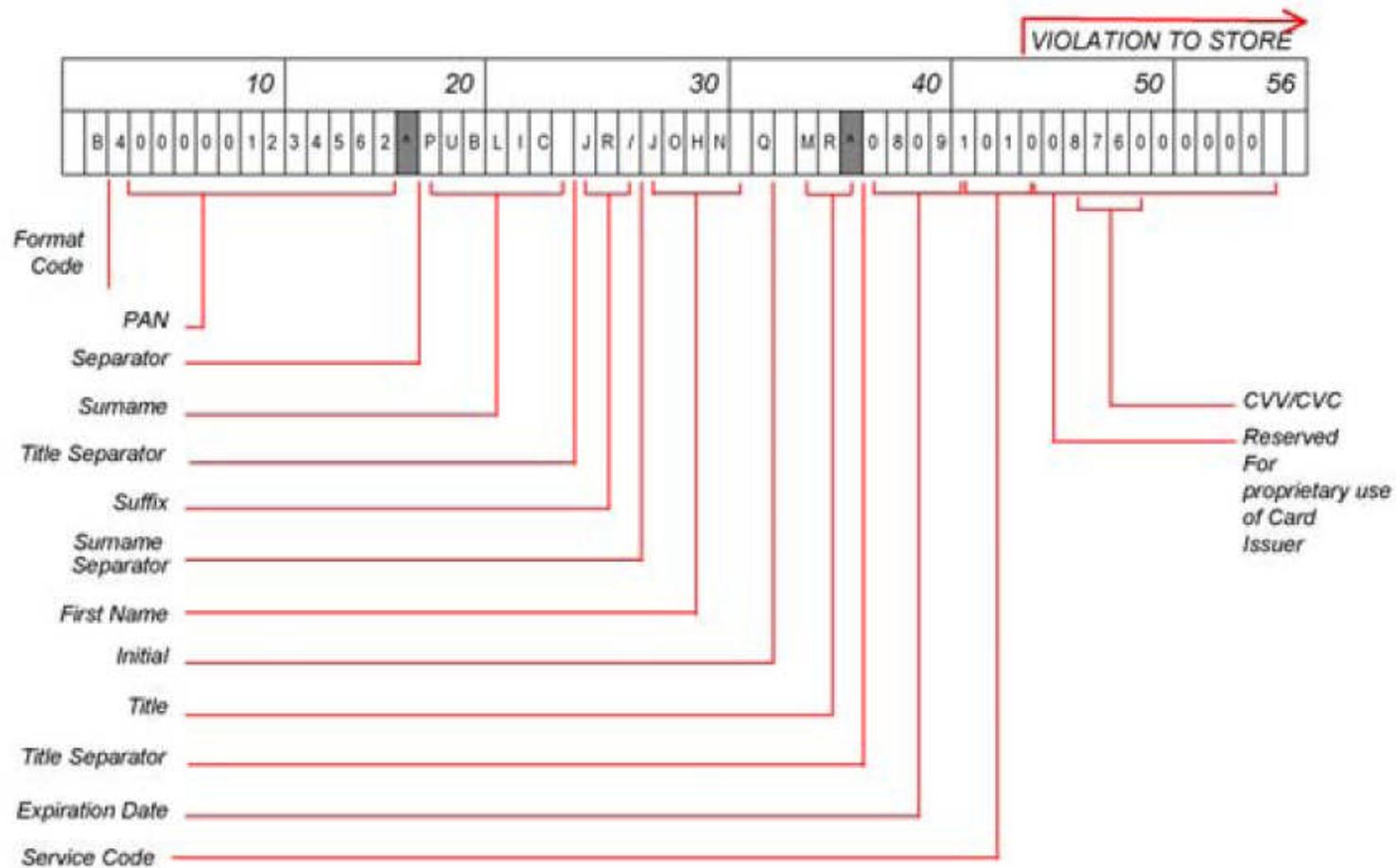


PCI prohibits merchants or their agents from storing the magnetic-stripe data after the response to the authorization request has been received.

Due to the serious nature of compromising cardholder data, Card Associations have implemented **substantial penalties** for non-compliance.

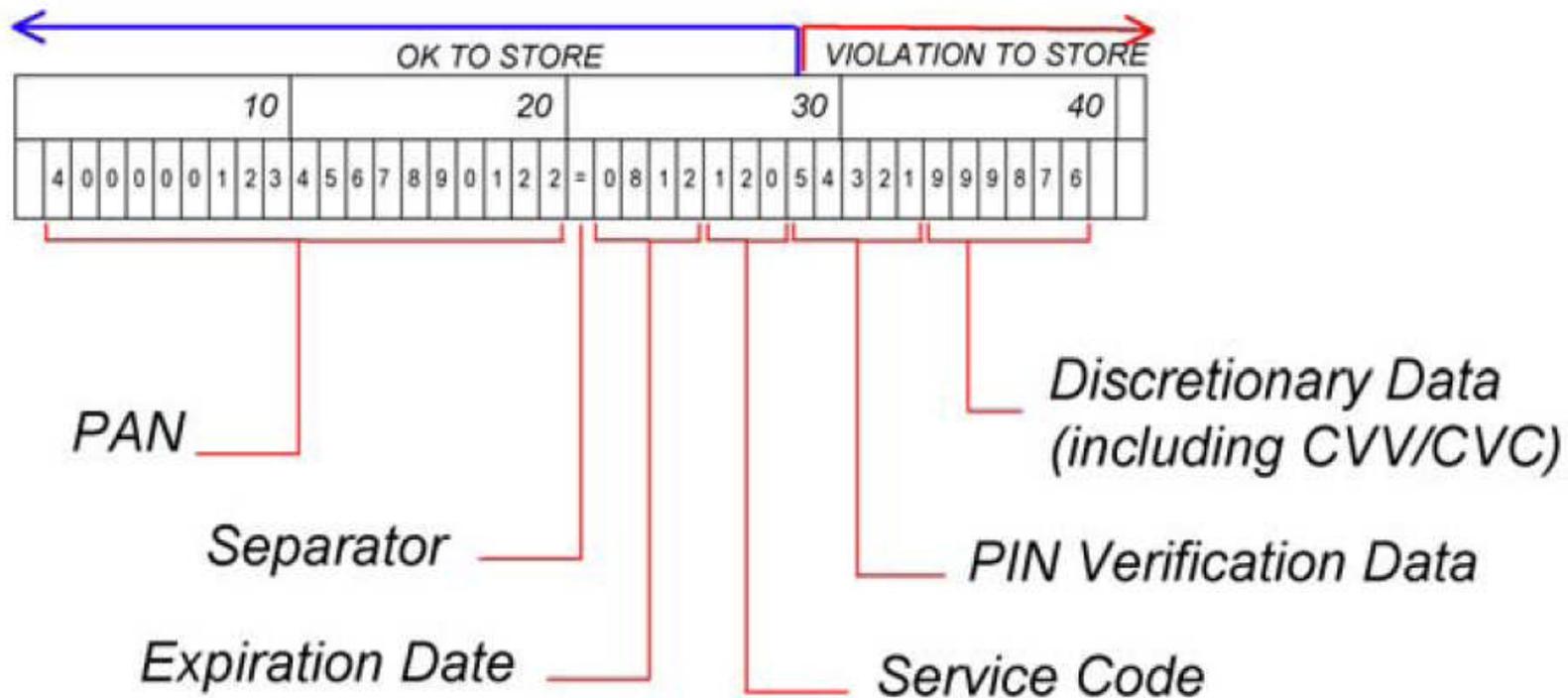
Track 1 Data

- Contains all fields of both track 1 and track 2
- Length up to 79 characters

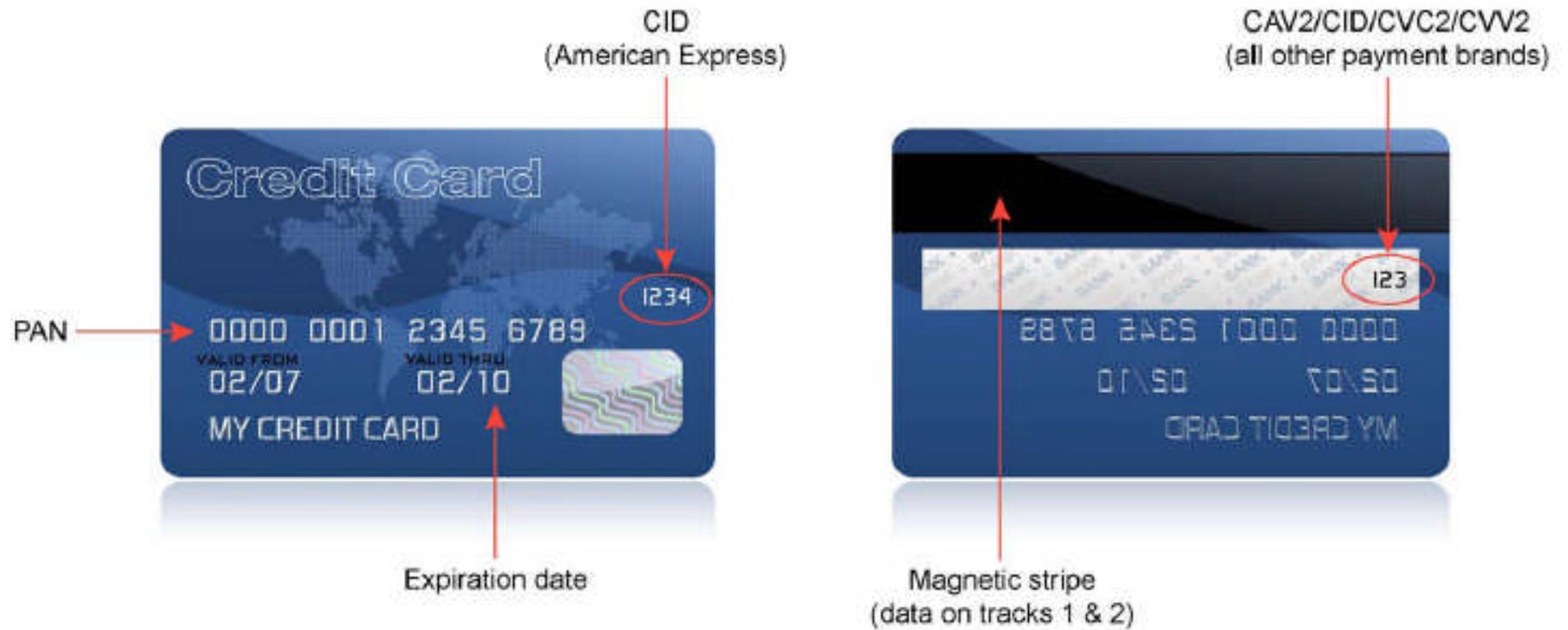


Track 2 Data

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters



CVV2



How do I know?

- Inventory all your data (including paper files).
- Search for *.log or *.txt
 - Focus on large files, or files which are generated periodically.
- Search key terms “Card” “CC” “Credit Card” “Batch”
- \windows\system32\logfiles directory with a focus on the W3SVC1
- Within all sampled files search for “^” and “=” to help identify track data.
- SQL queries “credit_card_data” “transaction_table”
- Search tools are available.

Coalfire's Navis and RapidSAQ

- Navis provides Coalfire customers with a robust suite of online tools to manage their IT governance and regulatory compliance programs.
- The platform allows you to not only manage compliance and audit plans, regulated assets, and controls, but also manage your Coalfire services and deliverables.
- Structured, interactive engine walks users through process and generates all appropriate documents
- Based on your responses Rapid SAQ:
 - Automatically determines the appropriate validation type (A, B, C or D) for the merchant
 - Presents only those required questions
 - Removes questions that are not appropriate
- Robust reporting with easy to read graphic stats
- Track your compliance against industry trends
- Can manage multiple entities from one management page (e.g. franchises and/or multiple locations)

Coalfire's Navis Platform

The screenshot shows a Windows Internet Explorer browser window displaying the Navis platform login page. The browser's address bar shows the URL <https://arm.coalfiresystems.com/Login.aspx?ReturnUrl=%2FDefault.aspx>. The page features the Navis logo and a 'Powered by Coalfire' badge. Below the logo are 'Login' and 'Register' buttons. The main content area is divided into three sections: a 'Welcome to Navis' section with introductory text and links to contact sales or register; a 'Coalfire Systems Information' section with a bulleted list of links; and a 'Login' section with input fields for 'User Name' and 'Password', a 'Login' button, and links for 'Forgot Your Password?' and 'Request Assistance?'. The footer contains the copyright notice '© 2008 Coalfire Systems, Inc. All rights reserved.'. The Windows taskbar at the bottom shows the Start button and several open applications: Navis - Windows Inte..., Inbox - Microsoft Out..., Calendar - Microsoft..., and Document2 - Microsof... The system tray on the right shows the Internet icon, a 135% zoom level, and the time 6:50 AM.

Navis - Windows Internet Explorer

<https://arm.coalfiresystems.com/Login.aspx?ReturnUrl=%2FDefault.aspx>

File Edit View Favorites Tools Help

Google G Go Bookmarks 27 blocked Check AutoLink AutoFill Send to Settings

Breaking News, Weather, Bu... Navis

Powered by **Coalfire**

Navis

Login Register

Welcome to Navis

Navis provides Coalfire customers with a robust suite of online tools to manage their IT governance and regulatory compliance programs.

The platform allows you to not only manage compliance and audit plans, regulated assets, and controls, but also manage your Coalfire services and deliverables.

[Click here to contact a Coalfire Sales representative today.](#)
[Click here to register for Coalfire Services.](#)

Coalfire Systems Information:

- [Home](#)
- [Industries](#)
- [Solutions & Services](#)
- [Resources & Tools](#)
- [Company Info](#)
- [News & Events](#)

Login

User Name:

Password:

Login

[Forgot Your Password?](#)

[Request Assistance?](#)

© 2008 Coalfire Systems, Inc. All rights reserved.

start Navis - Windows Inte... Inbox - Microsoft Out... Calendar - Microsoft... Document2 - Microsof... Internet 135% 6:50 AM



What are Quarterly Network Scans?

PCI Scanning Procedures v1.2

- Quarterly vulnerability scans (both internal and external) are required by PCI DSS 11.2
- External vulnerability scans are conducted over the Internet and required to be performed by an ASV.
- Internal vulnerability scans must be conducted against all CDE systems and can be done by internal IT staff.
- These scans are an indispensable tool to be used in conjunction with a vulnerability management program. Scans help identify vulnerabilities and miss-configurations of web sites, applications, and information technology (IT) infrastructures.
- Scan results provide valuable information that support efficient patch management and other security measures that improve protection against Internet and internal attacks.

PCI Scanning Procedures v1.2

The PCI DSS requires all Internet-facing IP addresses as well as internal CDE systems to be scanned for vulnerabilities.

In some instances, companies may have a large number of IP addresses available while only using a small number for card acceptance or processing. In these cases, ASV's can help merchants and service providers define the appropriate scope for the external scan required to comply with the PCI DSS.

What type of systems should be scanned?

1. Client provides the list of public IP addresses to scan to an ASV.
2. A network probe discovers live devices.
3. The IDS/IPS must not interfere with the scan
4. You must scan all:
 1. Web Servers
 2. Application and Database Servers
 3. Domain Name Servers
 4. Mail Servers
 5. All Virtual Hosts
 6. Wireless Access Points
 7. Routers and Firewalls
 8. Operating Systems

Sample Report



Executive Summary

Coalfire Systems, Inc (Coalfire) has determined that the State of Mississippi - [REDACTED] is **COMPLIANT** with the PCI scan validation requirement.

This report was generated by a PCI Approved Scanning Vendor, Coalfire Systems, under certificate number 3782-01-02, within the guidelines of the PCI data security initiative.

An external vulnerability assessment of the State of Mississippi - [REDACTED] was performed for all systems within project scope. The purpose of this assessment was to identify accessible systems and vulnerabilities on these systems from an untrusted network location, such as the Internet. Identification of these vulnerabilities allows the organization to measure itself against the PCI security program and take proactive remediation actions to maintain adequate protection of cardholder data.



Sample Report

Summary of Compliance Status

PCI DSS Compliance Statuses of live IP addresses within project scope are listed in the table below. The live IP addresses **do meet** minimum security standards as defined by the PCI security program. Non-reporting IP addresses within project scope are listed in the **Full IP Assessment Scope** section of this report.

PCI DSS Compliance Statuses

Overall VISA CISP Compliance Status		Pass
Live IP Address Scanned	Security Risk Rating	VISA CISP Compliance Status
.194	-	Pass
.195	2.6	Pass
.196	-	Pass
.197	-	Pass
.198	-	Pass
.200	-	Pass
.201	5.0	Pass
.202	-	Pass
.203	-	Pass

Vulnerability Severity Levels

Level	Severity	Description
5	Urgent	Trojan Horses; file read and writes exploit; remote command execution
4	Critical	Potential Trojan Horses; file read exploit
3	High	Limited exploit of read; directory browsing; DoS
2	Medium	Sensitive configuration information can be obtained by hackers
1	Low	Information can be obtained by hackers on configuration

How are scans ranked?

National Vulnerability Database CVSS Scoring - Windows Internet Explorer

http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

File Edit View Favorites Tools Help

NVD National Vulnerability Database CVSS Scoring

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists Product Dictionary Impact Metrics Data Feeds Statistics

Home ISAP/SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Common Vulnerability Scoring System Version 2 Calculator

This page provides a calculator for creating [CVSS](#) vulnerability severity scores. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores.

[Reset Scores](#) [View Equations](#)

CVSS Base Score	Undefined
Impact Subscore	Undefined
Exploitability Subscore	Undefined
CVSS Temporal Score	Undefined
CVSS Environmental Score	Undefined
Overall CVSS Score	Undefined

Base Score Metrics

Exploitability Metrics

Environmental Score Metrics

General Modifiers

CollateralDamagePotential

TargetDistribution

Impact Subscore Modifiers

ConfidentialityRequirement

IntegrityRequirement

AvailabilityRequirement

Technical and Operational Requirements for ASV's

Non-disruptive Nature of the ASV Solution

ASV solutions must provide only tests that do not damage the customers' systems or data. Solutions must not cause an activity that would result in a system reboot, or interfere with or change domain name server (DNS), routing, switching, and address resolution. Root-kits or other software must not be installed unless part of the solution and pre-approved by the customer.

The following are examples of some of the tests that are not permitted:

- Denial of service (DoS)
- Buffer overflow exploit
- Brute-force attack resulting in a password lockout
- Excessive usage of available communication bandwidth

But there are still risks with scans

- Routers/Firewalls
 - Some can't handle the traffic and have to be reset resulting in the network going down.
- Operating Systems
 - Some systems are built off older systems (like NT) and may react strangely to scans (i.e. VOIP systems).
- Custom Web Application Checks (XSS, SQL)
 - Scanning solutions are becoming more sophisticated at checking application vulnerabilities. Web spidering, and SQL injection tests may lead to denial-of-service type experiences.

Key Points

- Under what circumstance you can store sensitive authentication data post authorization?
- What is “sensitive authentication data”?
- How can you search for sensitive authentication data?
- What is the difference between the DSS, SAQ, and scans?

End of Session 2

Next up... Application Security

