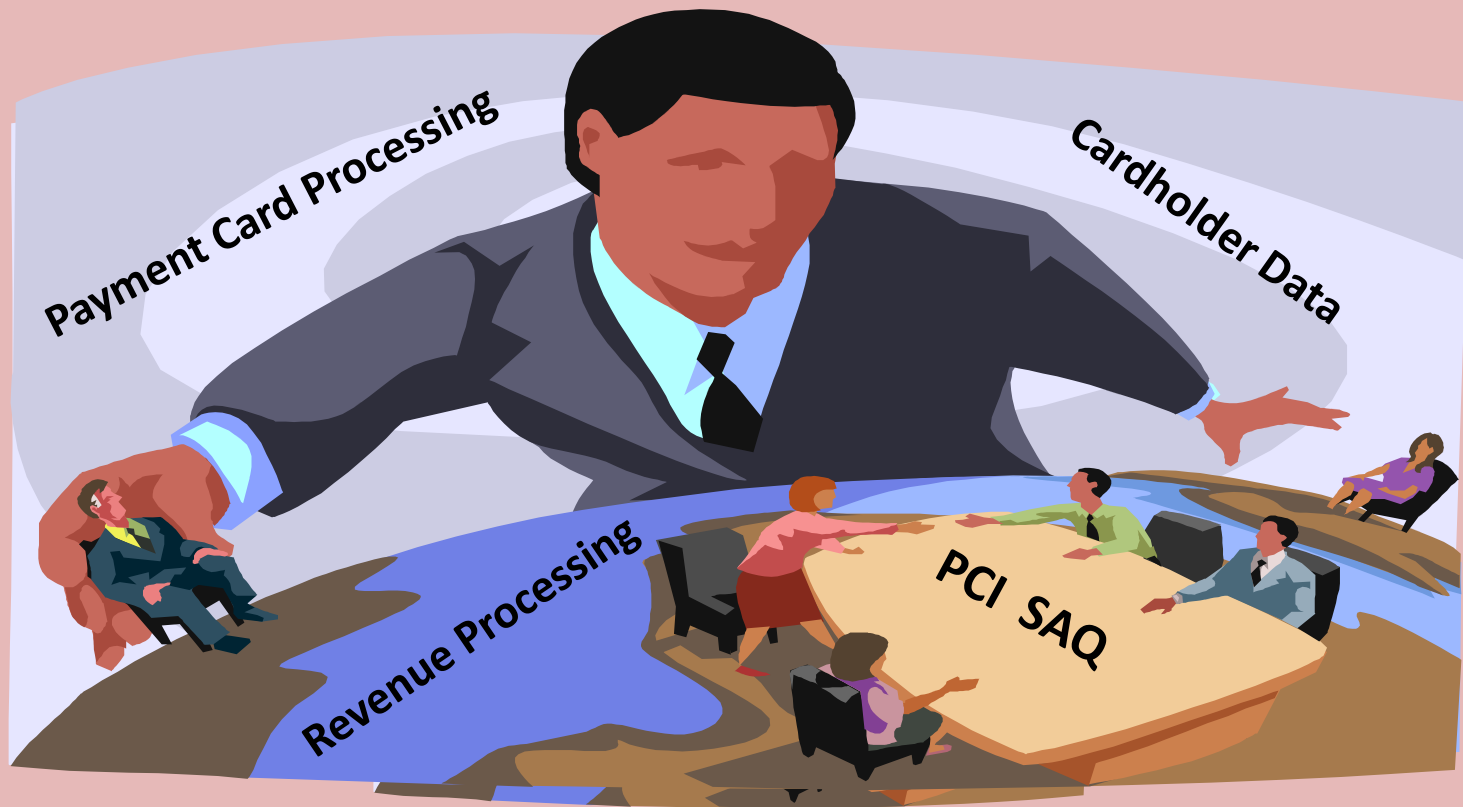


Annual Trustwave PCI Self Assessment Questionnaire (SAQ) Educational Presentation

**Understanding the Merchants
Responsibilities for PCI Compliance**

Agenda

- **Discussion on Merchant Responsibilities**
- **Discussion on SAQ's**
- **Discussion on New Expectations**
- **Question and Answer**



Merchant Responsibilities

PCI Merchant Responsibilities

Know your payment card processing business and how you process credit cards

- Mail, Phone, Online, Over the Counter F2F, Secure fax

24/7 adherence to PCI DSS

- Read PCI DSS standards
- Keep cardholder data secure and confidential
- Limit physical access to terminals and data from terminals; need to know basis

Attend Trainings; includes all employees who have access to cardholder data or revenue

- Revenue Process (attendance once every two years)
- Security Awareness Education (SAE-annually)

Complete Annual SAQ to attest PCI Compliance

PCI DSS Standards



AT A GLANCE
STANDARDS OVERVIEW

Payment Card Industry Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI Standards Include:

PCI Data Security Standards The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

PIN Transaction Security Requirements The PCI PTS applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

Payment Application Data Security Standards The PA-DSS is for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. It governs those applications that are sold, distributed or licensed to third parties.

PCI SSC Founders



PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Participating Organizations

Merchants, banks, processors, developers and point-of-sale vendors



S.A.Q.

SELF ASSESSMENT QUESTIONNAIRE

Self Assessment Questionnaire

Why do I have to complete the SAQ?

- Annual requirement for merchants that accept credit cards.
- Confirms that your department strives to keep cardholder data secure.
- Helps Treasury uncover possible weaknesses in processes that may violate PCI DSS.

Self Assessment Questionnaire

Most importantly you are attesting that your department is keeping your payment card processing environment secure by following the guidelines/policies set forth by the PCI Council and the IU Treasurers Office.

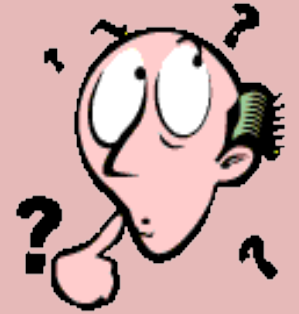


Self Assessment Questionnaire

Who should be completing the SAQ?

- Someone designated by Fiscal Officer
- Someone knowledgeable about the merchants processing environment
- Someone who has completed the SAE & Revenue Process Training

Which SAQ Should I Complete?



SAQ Description

- A-** Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
- B-** Standalone, dial-out merchants with no electronic cardholder data storage, imprint only merchants with no electronic cardholder data storage.
- C-VT-** Merchants using only web-based virtual terminals, no electronic cardholder data storage. (No IU Merchants)
- C-** Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. (No IU Merchants)
- D-** All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment card brand as eligible to complete an SAQ.

Which SAQ Should I Complete?

- SAQ's are based on merchant numbers.
- Each merchant number has to have an SAQ completed.
- Some departments have multiple payment card acceptance methods each having its own merchant number:
 - **Online**=IU PAY Plus, VeriSign/PayPal, Specialty Systems (ticketing, dining, parking, etc.)
Caution: No merchant should be entering cardholder data into an online system for the cardholder (i.e. No IU Computer or Workstation).
 - **POS Stand Alone Terminals** = F2F, Mail, Phone, Secure Fax
Caution: Any mail-in, phone-in, secure fax cardholder data should be cross shredded after entered into terminal. Email and phone messages strictly prohibited. Secure Fax acceptable.

Self Assessment Questionnaire

THE BASICS



Expiration Date








How many SAQ's







SAQ Type

SAQ (A) & B Merchants






Section A. ELIGIBILITY

Status	Item	Question	Your Response	Best Response	Comment
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:					
	0	Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions <small>[TWQ1923]</small>			<p>If you are using a 3rd party processor all credit card information is directly transacted on their site. If your department is entering cardholder data through your computers, STOP ! Consult with Treasury you may be in violation of PCI DSS.</p>
	1	The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant <small>[TWQ1924]</small>			
	2	Merchant does not store any cardholder data in electronic format. <small>[TWQ1926]</small>			
	3	Merchant retains only paper reports or receipts with cardholder data, and such documents are not received electronically <small>[TWQ1925]</small>			








SAQ A & (B) Merchants

Section A. ELIGIBILITY					
Status	Item	Question	Your Response	Best Response	Comment
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:					
	0	Merchant Description [TWQ1693]	Merchant uses only standalone, dial-up terminals; and the standalone, dial-up terminals are not connected to the Internet or any other systems within the merchant environment		Every merchant should be using a Treasury issued terminal. These terminals do not store cardholder data. The receipts that come out of them should be truncated and are not consider to be received electronically.
	1	Merchant does not store any cardholder data in electronic format. [TWQ1926]			
	2	Merchant retains only paper reports or receipts with cardholder data, and such documents are not received electronically [TWQ1925]			

SAQ B Merchants









Section B. 3. STORED DATA PROTECTION						
Status	Item	Question	Your Response	Best Response	Comment	
	B -1	Do all <i>s</i> ystems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)? (SAQ #3.2) <small>(TWQ2128)</small>			<p>This section is based on your POS terminal. A printout of terminal receipt and detail report should reveal the truncation of credit card and expiry date.</p>	
Do all <i>s</i> ystems adhere to the following requirements (answer "Yes" if you meet these requirements)?						
	4	Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, contained in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. <small>(TWQ2130)</small>				
	5	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (SAQ #3.2.2) <small>(TWQ2132)</small>				
	6	Do not store the personal identification number (PIN) or the encrypted PIN block.(SAQ #3.2.3) <small>(TWQ2134)</small>				
	B -5	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)? <small>(TWQ2136)</small>				

SAQ A & (B) Merchants








Section C. 4. TRANSMITTED DATA PROTECTION					
Status	Item	Question	Your Response	Best Response	Comment
	C-1	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)? (SAQ #4.2) <small>(TWQ2158)</small>			
Section D. 7. ACCESS RESTRICTIONS					
Status	Item	Question	Your Response	Best Response	Comment
	D-1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access? (SAQ #7.1) <small>(TWQ2200)</small>			
Section E. 9. PHYSICAL ACCESS CONTROLS					
Status	Item	Question	Your Response	Best Response	Comment
	E-1	Are all paper and electronic media that contain cardholder data physically secure? (SAQ #9.6) <small>(TWQ2246)</small>			
	E-2	Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?(SAQ #9.7.a) <small>(TWQ2248)</small>			
Do controls include the following:					
	12	Is the media classified so it can be identified as confidential?(SAQ #9.7.1) <small>(TWQ2250)</small>			

P P P should be written using the sections of the SAQ as the outline. Give detail descriptions for each section of how your department handles and/or maintains the information referenced in each question.

SAQ A & B Merchants



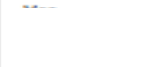







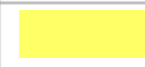



Section E. 9. PHYSICAL ACCESS CONTROLS					
Status	Item	Question	Your Response	Best Response	Comment
	13	Is the media sent by secured courier or other delivery method that can be accurately tracked?(SAQ #9.7.2) <small>(TWQ2252)</small>			<p>This section is asking how you control the physical access to cardholder data, how is it transmitted, secured, and destroyed after it is no longer needed.</p>
	E -6	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)? (SAQ #9.8) <small>(TWQ2254)</small>			
	E -6	Is strict control maintained over the storage and accessibility of media that contains cardholder data? (SAQ #9.9) <small>(TWQ2256)</small>			
	E -7	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows: (SAQ #9.10) <small>(TWQ2260)</small>			
	E -8	Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? (SAQ #9.10.1) <small>(TWQ2262)</small>		Y	
Section F. 12. SECURITY POLICIES AND PROCEDURES					
Status	Item	Question	Your Response	Best Response	
	F -1	Is a security policy established, published, maintained, and disseminated? (SAQ #12.1) <small>(TWQ2299)</small>			
Does the security policy accomplish the following:					

SAQ A & (B) Merchants

Section F. 12. SECURITY POLICIES AND PROCEDURES					
Status	Item	Question	Your Response	Best Response	Comment
	19	Includes a review at least once a year and updates when the environment changes?(SAQ #12.1.3) <small>(TWQ2303)</small>			
	F -3	Are usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all employees and contractors?(SAQ #12.3.a) <small>(TWQ2306)</small>		1	
	F -4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?(SAQ #12.4) <small>(TWQ2318)</small>			
Are the following information security management responsibilities assigned to an individual or team? (Note: T needs not necessarily perform all the tasks related to the particular area of responsibility, but they can delegate accountable for their area of responsibility.)					
	22	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?(SAQ #12.6.3) <small>(TWQ2322)</small>			
	F -6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?(SAQ #12.6) <small>(TWQ2326)</small>		1	
	F -7	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following? (SAQ #12.8) <small>(TWQ2331)</small>		1	







This section contains questions that pertain to your department and to Treasury functions. Your PPP should include what you do in your department in regards to these security questions. Treasury is available to consult with you concerning this section and the writing of your PPP's.

SAQ A & B Merchants

Section F. 12. SECURITY POLICIES AND PROCEDURES					
Status	Item	Question	Your Response	Best Response	Comment
	Do policies and procedures include the following:				
	25	A list of service providers is maintained. (SAQ #12.8.1) <small>[TWQ2333]</small>			<div style="border: 2px solid blue; border-radius: 20px; padding: 10px;"> <p>These next four questions in particular relate to the functions that Treasury maintains and we will add the documentation to each merchant's Virtual Binder.</p> </div>
	26	A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. (SAQ #12.8.2) <small>[TWQ2335]</small>			
	27	There is an established process for engaging service providers, including proper due diligence prior to engagement. (SAQ #12.8.3) <small>[TWQ2337]</small>			
	28	A program is maintained to monitor service providers' PCI DSS compliance status. (SAQ #12.8.4) <small>[TWQ2339]</small>			
Section G. CONFIRMATION AND ACKNOWLEDGEMENT					
Status	Item	Question	Your Response	Best Response	
	CA.1	PCI DSS Self-Assessment Questionnaire was completed according to the <small>[TWQ1918]</small>			
	CA.2	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment. <small>[TWQ1919]</small>			

SAQ A & B Merchants

Section G. CONFIRMATION AND ACKNOWLEDGEMENT

Status	Item	Question	Your Response	Best Response	Comment
	CA.3	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times. (TWQ1920)		--	<p>This final section is your attestation that you understand what you just completed, that it is a full assessment of your payment card environment, and that you have read the PCI DSS. Whomever completes the SAQ will sign it.</p>
	CA.4	No evidence of magnetic stripe (i.e., track) data", CAV2, CVC2, CID, or CVV2 data", or PIN data" storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment. (TWQ1921)		Y	
	CA.5	I have confirmed with my POS vendor that my POS system does not store sensitive authentication data after authorization. (TWQ1922)		Y	
	CA.6	Signature of Executive Officer (please provide full name) (TWQ1924)	--		
	CA.7	Title of Executive Officer (TWQ1923)	Manager		

Compliance Certificate



PCI DSS Certificate of Compliance

Certificate Number: 4F71-D742-42EE-0359

Awarded To: **Treasury web Testing (IU PAY)**

PCI Level: 4
Classification: Merchant
Expiration Date: Oct 11, 2011

Trustwave Engagement Information

Self-Assessment Questionnaire: Pass
Date Completed: Oct 12, 2010
Version Completed: PCI 1.2 - Form A
Client SAQ Abbreviation: Kim L Stuart
Title: Senior Mgr. Treasury Ops.

Client Authorization: _____
Print Name Sign Name

This signed order of Treasury web Testing (IU PAY) agrees to the accuracy of all information provided within TrustCenter.

To maintain compliance this order must remain signed and sealed as an "OIG" (Original) Certificate of an outside agency. This is subject to the terms and conditions of the Payment Card Industry Security Standards Council and the payment card brands. For information on applying for the 2010 PCI DSS Self-Assessment Questionnaire (SAQ), visit www.pcisecuritystandards.org. In addition, PCI DSS Self-Assessment Questionnaire (SAQ) 1.2-Form A is available for download from the Payment Card Industry Security Standards Council website. For additional information, visit www.pcisecuritystandards.org. This certificate is valid for the duration of the assessment period. It is the client's sole responsibility to ensure compliance with the certification security requirements and to be validated by PCI DSS.

This certificate is for the sole purpose of identifying compliance with PCI DSS and is not intended to be used for any other purpose. This certificate is for the sole purpose of identifying compliance with PCI DSS and is not intended to be used for any other purpose. This certificate is for the sole purpose of identifying compliance with PCI DSS and is not intended to be used for any other purpose.

Trustwave is a registered provider of PCI DSS Self-Assessment Questionnaire (SAQ) 1.2-Form A. Trustwave is a registered provider of PCI DSS Self-Assessment Questionnaire (SAQ) 1.2-Form A.

Trustwave © 2010



Compliance Certificate

PRINT

- Print certificate after completion of SAQ

SIGN

- Sign and date certificate
- Signatures required: person completing SAQ & Fiscal Officer

FORWARD

- Forward to Treasury Operations Office
- Treasurers Office signs certificate to verify SAQ completion

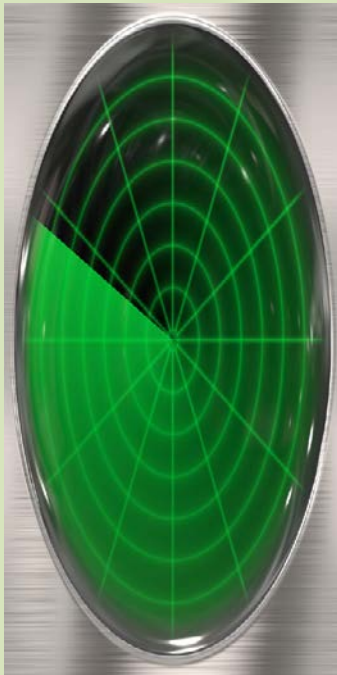
SAQ D Merchants

The Sections of SAQ D

- A) Firewall Configuration
- B) Systems Settings
- C) Stored Data Protection
- D) Transmitted Data Protection
- E) Anti-Virus Protection
- F) Application & Systems Security
- G) Access Restrictions
- H) Account Security
- I) Physical Access Controls
- J) Access Tracking
- K) Monitoring & Testing
- L) Security Policies & Procedures
- M) Hosting Providers
- N) Confirmation & Acknowledgement

SAQ D Merchants

Beyond The Basics



PCI Vulnerability Scans

- Monthly
- Log Results
- Complete Scan Attestation

Trustwave Scan Report Attestation of Compliance

Trustwave Scan Report Attestation of Compliance

Scan Customer Information		Approved Scanning Vendor Information	
		Company: Trustwave	
Contact: Ranji Abraham	Title	Contact: Trustwave Support	Email: support@trustwave.com
Telephone:	Email: abraham@indiana.edu	Telephone: 1-800-363-1621 (US Toll free) or +1-312-267-3212 (US Toll) or +44 (0) 845 456 9613 (UK Toll Free)	
		Business Address: 70 West Madison St., Ste 1050	
City:	State/Province: IN	City: Chicago	State/Province: Illinois
Zip: 47405	Country: US	Zip: 60602	Country: USA
URL:		URL: www.trustwave.com	

Scan Status:

- Compliance Status: **Pass**
- Number of unique components scanned: 2
- Number of identified failing vulnerabilities: 0
- Number of components not scanned by TrustKeeper because the customer confirmed they were out of scope: 0
- Date scan completed: Jul 13, 2011
- Scan expiration date (3 months from date scan completed): Oct 13, 2011

Scan Customer Attestation

RPS Dining Services - Server A attests that: "This scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. RPS Dining Services - Server A also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS; This scan does not represent RPS Dining Services - Server A's overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements."

Signature

Name

Title

Date

ASV Attestation

This scan and report were prepared and conducted by Trustwave under certificate number 3702-01-05, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.

Trustwave Scan Report Attestation of Compliance



Executive Summary Scan Report

This report was generated by the PCI Approved Scanning vendor Trustwave, under certificate number 3702-01-05 within the guidelines of the PCI data security initiative.

Trustwave has determined that RPS Dining Services - Server A is COMPLIANT with the PCI scan validation requirement.

The TrustKeeper scan examines your systems for vulnerabilities and policy violations according to the PCI Standard. This report summarizes the Compliance Status and any identified issues. Please refer to the Audit Report for the detailed information from which this summary was derived. The audit report reflects the full and authoritative compliance data for this assessment.

Part 1. Scan Information

Scan Customer Company: RPS Dining Services - Server A

ASV Company: Trustwave

Date scan was completed: Jul 13, 2011

Scan Expiration Date: Oct 13, 2011

Part 2. Component Compliance Summary

Systems Scanned

#	Status	IP Address
1.	- Pass	140.182.33.38

Vulnerabilities

Falling	Compromise	High	Medium	Low	Informational
					4

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Repealed Vulnerabilities (Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability)
140.182.33.38	SSL Certificate is Not Trusted	I	0.00	Pass	
140.182.33.38	OV/DV Certificate Detected	I	0.00	Pass	
140.182.33.38	Discovered HTTP Methods	I		Pass	

Trustwave Scan Report Attestation of Compliance



Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address	Severity Level	CVSS Score	Compliance Status	Repealed Vulnerabilities (Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability)
140.182.33.38	Windows Terminal Services	I		Pass	

Consolidated Solution/Correction Plan for above IP Address:

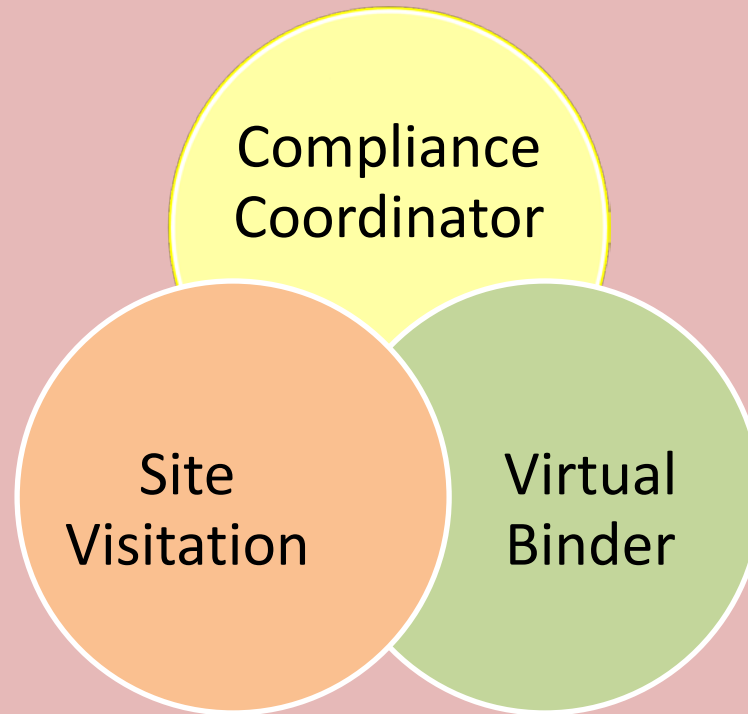
Part 3b. Special Notes by IP Address

IP Address	Note	Item Noted	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
No Special Notes				



New Expectations

Interconnected PCI Relationship



Equals a PCI Compliant Environment

PCI Compliance Coordinator

Responsibilities

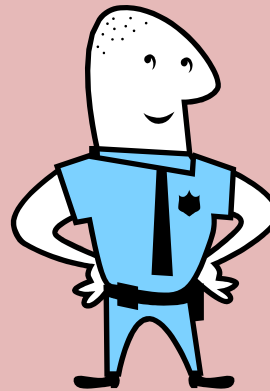
- Complete annual SAQ
- Maintain Virtual Binder
- Primary Contact for PCI
- Maintain, update, all employee training which includes:

Security Awareness Education (SAE)

Revenue Process Training

Qualifications

- ✓ Prefer full-time employee
- ✓ Trained
SAE & Revenue Process



Virtual PCI Binder

❖ **SharePoint Environment – all documents will be virtual**

❖ **Binder Contents:**

Departments PCI policies and procedures

PCI Compliance Certificate-Treasury adds

Signed Merchant Agreement-Treasury adds

Copy of Terminal receipt

Copy of applications, brochures, paper forms requesting credit card info

3rd Party Service Provider Info-Treasury adds

Employee List of trainings completed

Equipment spec sheets-Treasury adds

Visio diagrams

Firewall rules

IP addresses

Gateways used

Vulnerability Scan dates & results

SAQ D-Additional contents

Site Visitations

Treasury will conduct periodic site visits to validate ongoing adherence with PCI DSS which will consist of:

- Comparison of Virtual Binder to daily environmental processes and activities.
- Review all aspects of your revenue processes, credit card, cash and checks.

Presenter
Kim L. Stuart, CTP
Senior Manager, Treasury Operations
Email: klstuart@indiana.edu
Phone: 812-856-5838



Questions and Answers