

Cloud Security Pros Unite – PCI DSS for 2014 and Beyond

*Kurt Hagerman
Director of Information Security*



*16th Annual New York State
Cyber Security Conference*

5 June, 2013



Agenda

- *Background on the PCI DSS and Service Providers*
 - *What makes a Service Provider?*
- *Service Provider Assessments*
 - *Pick your controls*
- *Current Attestation Documents*
 - *Report on Compliance*
 - *Attestation of Compliance*
 - *Changes to Attestation Documents*
- *Improving Visibility*
 - *What to ask potential providers*





The PCI DSS and Service Providers

- *The original definition of service provider*
 - *Any entity who plays a direct role in the transaction between the cardholder and the authorizing bank.*
 - *Typically included payment gateways, processors, fraud/chargeback services, clearing and settlement*
- *Revisions to the definition*
 - *Any entity who has an impact on the security of the cardholder data environment*
 - *Captured many more third parties providing services to merchants*
- *Cloud Hosting Providers and the PCI DSS*
 - *Widely varying scope of services*
 - *Similar claims of being “PCI Compliant”*



Service Provider Assessments

- *Pick your controls*
 - *Service providers are allowed to select which services they offer and which DSS controls are to be included in their assessment*
 - *Many took the shortest route to “PCI Compliance” by only including physical and personnel security controls (part of requirements 9 and 12)*
- *Inconsistent QSA led Assessments*
 - *Unclear guidelines from the Council to QSAs performing assessments*
 - *Not all assessments are created equal – not all assess both the service provider’s business as well as the services themselves*
 - *Documentation of the Report on Compliance (ROC) varies widely from the reporting instructions provided by the PCI Council.*





Current Attestation Documents

- Scoping section of the ROC incomplete or unclear
 - Must fully describe the CDE, what systems are in scope, what is excluded, what services are included along with requisite detail

3. Details about Reviewed Environment	
<p>Include the following details in this section:</p> <ul style="list-style-type: none"> • A diagram of each piece of the communication link, including LAN, WAN, or Internet 	<ul style="list-style-type: none"> • Identify each communication/connection point in scope. • Provide one or more detailed diagrams to illustrate each communication point. Diagrams should include the following: <ul style="list-style-type: none"> ○ All boundaries of the cardholder data environment ○ Any network segmentation points which are used to reduce scope of the assessment ○ Boundaries between trusted and untrusted networks ○ Wireless and wired networks ○ All other connection points applicable to the assessment • Ensure the diagram(s) include enough detail to clearly understand how each communication point functions and is secured. (For example, the level of detail may include identifying the types of devices, device interfaces, network technologies, protocols, and security controls applicable to that communication point.) <p><i>Note: This diagram or diagrams are additional to the high-level diagram provided in Section 1 and should provide a more detailed view of the communication points within the environment.</i></p>
<ul style="list-style-type: none"> • Description of cardholder data environment, for example: <ul style="list-style-type: none"> - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback, and other flows as applicable 	<ul style="list-style-type: none"> • Provide a detailed description of cardholder data environment, including the following. <ul style="list-style-type: none"> ○ Identify all transmission and processing flows of cardholder data, including: <ul style="list-style-type: none"> - Authorization - Capture - Settlement - Chargeback - Any other flows as applicable ○ For each transmission and processing flow: <ul style="list-style-type: none"> - Describe how cardholder data is transmitted and/or processed. - Identify the types of cardholder data involved (for example, full track, PAN, expiry date). <p><i>Note: Include all types of data flows, including any involving hard-copy/paper media. A combination of descriptions and data-flow diagrams may be helpful to illustrate this.</i></p>
<ul style="list-style-type: none"> - List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.): 	<ul style="list-style-type: none"> • Identify and list all databases, tables, and files storing cardholder data (including electronic and hard copy). • For each item in the list, provide the following information:



Current Attestation Documents

- *Attestation of Compliance (AOC) does not provide adequate detail*
- *Part 2a does not contain categories that clearly describe current hosting solutions*

Part 2 PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

<input type="checkbox"/> Payment Processing-POS	<input type="checkbox"/> Tax/Government Payments	<input type="checkbox"/> Fraud and Chargeback Services
<input type="checkbox"/> Payment Processing-Internet	<input type="checkbox"/> Payment Processing – ATM	<input type="checkbox"/> Payment Processing – MOTO
<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Payment Gateway/Switch	<input type="checkbox"/> Clearing and Settlement
<input type="checkbox"/> Account Management	<input checked="" type="checkbox"/> 3-D Secure Hosting Provider	<input type="checkbox"/> Loyalty Programs
<input type="checkbox"/> Back Office Services	<input type="checkbox"/> Prepaid Services	<input type="checkbox"/> Merchant Services
<input type="checkbox"/> Hosting Provider – Web	<input checked="" type="checkbox"/> Managed Services	<input type="checkbox"/> Billing Management
<input checked="" type="checkbox"/> Network Provider/Transmitter	<input checked="" type="checkbox"/> Hosting Provider – Hardware	<input type="checkbox"/>
<input checked="" type="checkbox"/> Records Management	<input type="checkbox"/> Data Preparation	<input type="checkbox"/>
<input type="checkbox"/> Others (please specify): <input type="text"/>		



Current Attestation Documents

- *Attestation of Compliance (AOC) does not provide adequate detail*
 - *Part 4 requires that all control categories be checked “Yes” for a compliant ROC even if whole or partial controls were excluded from the assessment*
 - *Misleads customers into believing the service provider is fully compliant*
 - *Does not provide clear differentiation between service providers offering different levels of service*



Current Attestation Documents

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Protect stored cardholder data.	<input type="checkbox"/> Yes <input type="checkbox"/> No	



Changes to Attestation Documents

- *Potential Changes to the Service Provider AOC*
 - *Add/change categories in Part 2a*
 - *Change guidance on use of Part 4*
- *Still an opportunity to weigh in on the AOC*
 - *SSC still working on revising the AOC*
 - *Provide direct feedback and/or ask your QSA to do the same*





Improving Visibility: What to ask your provider

- **ASK** for the scoping section of the ROC (*Report on Compliance*)
- **ASK** for a responsibility matrix and service descriptions
 - Should indicate for each control who owns responsibility or if it is shared
 - Service descriptions should clearly delineate all shared responsibilities
- **ASK** for other third party audit reports and attestations
 - SSAE 16 SOC 2 Type II
 - ISO/IEC 27001:2005
 - HITRUST CSF
- **ASK** for internal audit reports





Thank You

Questions?

Kurt Hagerman



Email *kurt.hagerman@firehost.com*

Phone *+1 877 262 3473 x8073*