



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.0

February 2014



Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Microsoft Azure	DBA (doing business as):	
Contact Name:	Lori Woehler	Title:	Principal Group PM Manager, Global Ecosystem @Compliance and Trust
ISA Name(s) (if applicable):	N/A	Title:	
Telephone:	(425) 882.8080	E-mail:	Lori.woehler@microsoft.com
Business Address:	One Microsoft Way	City:	Redmond,
State/Province:	WA	Country:	USA
		Zip:	98052-6399
URL:	www.azure.com		

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Neohapsis, Inc.		
Lead QSA Contact Name:	Willie Rushton	Title:	Senior Security Consultatnt
Telephone:	773-296-6300	E-mail:	wrushton@neohapsis.com
Business Address:	217 N. Jefferson, Suite 200	City:	Chicago
State/Province:	IL	Country:	USA
		Zip:	60661
URL:	www.neohapsis.com		



Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed: Azure Core Services, Platform Services, Directory Services, Data Processing, Infrastructure, Operations

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POS / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):

Account Management

Fraud and Chargeback

Payment Gateway/Switch

Back-Office Services

Issuer Processing

Prepaid Services

Billing Management

Loyalty Programs

Records Management

Clearing and Settlement

Merchant Services

Tax/Government Payments

Network Provider

Others (specify):

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.



Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed: N/A

Type of service(s) not assessed:

Hosting Provider:

- Applications / software
 Hardware
 Infrastructure / Network
 Physical space (co-location)
 Storage
 Web
 Security services
 3-D Secure Hosting Provider
 Shared Hosting Provider
 Other Hosting (specify):

Managed Services (specify):

- Systems security services
 IT support
 Physical security
 Terminal Management System
 Other services (specify):

Payment Processing:

- POS / card present
 Internet / e-commerce
 MOTO / Call Center
 ATM
 Other processing (specify):

Account Management

Fraud and Chargeback

Payment Gateway/Switch

Back-Office Services

Issuer Processing

Prepaid Services

Billing Management

Loyalty Programs

Records Management

Clearing and Settlement

Merchant Services

Tax/Government Payments

Network Provider

Others (specify):

Provide a brief explanation why any checked services were not included in the assessment:

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Microsoft Azure does not directly store, process, or transmit cardholder data

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

Microsoft provides Cloud services (Infrastructure as a Service(IaaS), and platform as a services (PaaS) that their clients may use to process, store, and transmit cardholder data

Part 2c. Locations

List types of facilities and a summary of locations included in PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.):

Type of facility:

Location(s) of facility (city, country):

Corporate offices

Redmond, WA

Data Centers

Northlake, IL, Des Moines, IA,

Data Centers

San Antonio, TX Santa Clara, CA, Bristow, Boydton & Ashburn, VA

Data Centers

Amsterdam Netherlands, Dublin, Ireland



Data Centers	Hong Kong, China, Singapore

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? Yes No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

Network and system components that support Azure clients. Azure does not directly store process, or transmit cardholder data.

Does your business use network segmentation to affect the scope of your PCI DSS environment?
(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

Yes
 No

Part 2f. Third-Party Service Providers

Does your company have a relationship with one or more third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

Yes
 No

If Yes:

Type of service provider:	Description of services provided:
Microsoft Global Foundation Services	Network and Data Center management

Note: Requirement 12.8 applies to all entities in this list.



Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Azure Core Services, Azure Platform Services, Azure Directory Services, Data Processing, Infrastructure, Operations		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>1.1.3.a Azure does not store process or transmit, or have access to cardholder data environments.</p> <p>1.2.3 Microsoft Azure does not have wireless technologies within their production environment and does not store, process or directly transmit cardholder data.</p> <p>1.3.7 Wireless is not deployed within the Microsoft Azure Environment</p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>2.1.1.a Wireless is not deployed within the Microsoft Azure</p> <p>2.1.1.b Wireless is not deployed within the Microsoft Azure</p> <p>2.1.1.c Wireless is not deployed within the Microsoft Azure</p> <p>2.1.1.d Wireless is not deployed within the Microsoft Azure</p> <p>2.1.1.e Wireless is not deployed within the Microsoft Azure</p> <p>2.2.2.b No insecure services are enabled</p> <p>2.2.3 No insecure services are enabled</p>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>3.1.1.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.1.1.b Microsoft Azure does not store, process, or directly transmit cardholder data</p>



				<p>3.1.1.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.1.1.d Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.1.1.e Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.2.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.2.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.2.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.2.d Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.3 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.3.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.3.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.3.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.1.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.1.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.1.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.4.d Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.5 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.5.1 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.5.2.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.5.2.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.1 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.2 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.3 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.4 Microsoft Azure does not store, process, or</p>
--	--	--	--	---



				<p>directly transmit cardholder data</p> <p>3.6.5.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.5.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.5.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.6 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.7 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.8 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>3.6.b Microsoft Azure does not store, process, or directly transmit cardholder data</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>4.1.1 Windows Azure does not allow wireless network transmitting, or access to, cardholder data.</p> <p>4.1 Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.b Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.c Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.d Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.e Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.f Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.1.g Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.2.a Microsoft Azure does not store, process, or directly transmit cardholder data</p> <p>4.2.b Microsoft Azure does not store, process, or directly transmit cardholder data</p>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.9 Microsoft Azure does not process payment transactions</p> <p>9.9.1 Microsoft Azure does not have POS payment transactions</p>



				<p>9.9.1.a Microsoft Azure does not have POS payment transactions</p> <p>9.9.1.b Microsoft Azure does not have POS payment transactions</p> <p>9.9.2.a Microsoft Azure does not have POS payment transactions</p> <p>9.9.3.a Microsoft Azure does not have POS payment transactions</p> <p>9.9.3.b Microsoft Azure does not have POS payment transactions</p> <p>9.9.10 Microsoft Azure does not have POS payment transactions</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.5.5 All logs are forwarded to a centralized logging server. The logging storage solution does not allow users to change any logging entries.
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>12.7 Windows Azure does not have any personnel with access to cardholder data based on the architecture of their environment.</p> <p>12.8.1 Windows Azure does not store, process, or Share Cardholder data.</p> <p>12.8.2 Windows Azure does not have access to cardholder data and does not share cardholder data with external entities.</p> <p>12.9.5 Windows Azure network architecture prohibits wireless networks from being introduced into the network in a manner that could affect the cardholder data environment.</p> <p>12.3.10.b Windows Azure does not Store, or Process Cardholder data</p>
Appendix A:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	<i>December 31, 2014</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *December 31, 2014*, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of (date): (**check one**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Microsoft Azure</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures, Version 3.0</i> , and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



Part 3a. Acknowledgement of Status (continued)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys</i> |

Part 3b. Service Provider Attestation

<div style="border: 1px solid blue; padding: 2px;"> <p style="color: blue; font-size: small;">E8CB738B0575462</p> <p><i>Lori L. Woehler</i></p> <p style="color: blue; font-size: small;">DocuSigned By: Lori L. Woehler</p> </div>	
Signature of Service Provider Executive Officer	Date: 2/9/2015
Service Provider Executive Officer Name: Lori Woehler	Title: Principal Group PM Manager, Global Ecosystem @Compliance and Trust

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	<i>The QSA performed the assessment of in-scope PCI v 3.0 requirements for compliance</i>
<div style="border: 1px solid blue; padding: 2px;"> <p style="color: blue; font-size: small;">DocuSigned by:</p> <p><i>James Mobley</i></p> <p style="color: blue; font-size: small;">94EF7211287C4G1...</p> </div>	
Signature of QSA	Date: 2/6/2015
QSA Name: James Mobley, Authorized Officer	QSA Company: Neohapsis, Inc.

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	<i>N/A</i>
Signature of ISA	Date:
ISA Name:	Title:

¹ Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

