Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

PCI Security Standards Council

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 Cloud & Enterprise – Azure Services		DBA (doing business as):	Not Applicable	
Contact Name:	Alice Rison		Title:	Principal Group PM Manager	
ISA Name(s) (if applicable):	Not Applicable		Title:	Not Applicable	
Telephone:	425-707-2570 x72570		E-mail:	alrison@microsoft.com	
Business Address:	One Microsoft Way		City:	Redmond	
State/Province:	WA	Country:	USA	Zip:	98052
URL:	https://www.azure.microsoft.com				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Deepa Saldanha		Title:	Senior Director, QSA	
Telephone:	303-554-6333		E-mail:	pciqa@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	www.coalfire.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:	The following Microsoft Azure services are in scope and were assessed as part of the Microsoft C&E offering:
	
	Customer Facing Services
	• Azure IoT Hub
	• Active Directory Device Registration
	• Service Fabric
	• StorSimple
	• API Management
	• Operations Management Suite (OMS)
	  o Azure Automation
	  o Log Analytics
	  o Azure Backup
	  o Azure Site Recovery
	• Microsoft Intune
	• Azure Container Service
	• Azure Stream Analytics
	• Power BI
	• Storage Resource Provider
	
	Internal Infrastructure Supporting the Platform and Azure Services
	• OneDDOS
	• OneDeploy Express V2
	• Service Fabric RP Cluster

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☒ Applications / software	☒ Systems security services	☐ POS / card present
☒ Hardware	☒ IT support	☐ Internet / e-commerce
☒ Infrastructure / Network	☒ Physical security	☐ MOTO / Call Center
☒ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☒ Storage	☐ Other services (specify):	☐ Other processing (specify):
☒ Web		
☒ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		

- ☐ Account Management
- ☐ Back-Office Services
- ☐ Billing Management
- ☐ Clearing and Settlement
- ☐ Network Provider
- ☐ Others (specify):
- ☐ Fraud and Chargeback
- ☐ Issuer Processing
- ☐ Loyalty Programs
- ☐ Merchant Services
- ☐ Payment Gateway/Switch
- ☐ Prepaid Services
- ☐ Records Management
- ☐ Tax/Government Payments

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:	Not Applicable

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
- ☐ Back-Office Services
- ☐ Billing Management
- ☐ Clearing and Settlement
- ☐ Network Provider
- ☐ Others (specify):
- ☐ Fraud and Chargeback
- ☐ Issuer Processing
- ☐ Loyalty Programs
- ☐ Merchant Services
- ☐ Payment Gateway/Switch
- ☐ Prepaid Services
- ☐ Records Management
- ☐ Tax/Government Payments

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

PCI Security Standards Council

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Microsoft Azure is a cloud service provider, offering hardware, infrastructure, and computing platforms for building, deploying, and managing applications and services. Microsoft Azure does this through a global network of Microsoft Corporation and third-party managed datacenters. Microsoft Azure supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings. Microsoft Azure product offerings are designed to meet their customers' security, privacy, and compliance requirements. Microsoft Azure physical infrastructure is owned and managed by Microsoft Cloud Infrastructure and Operations (MCIO). Microsoft Azure doesn't directly store, process, or transmit card holder data (CHD); however, their tenant customers have the ability to operate ecommerce, and financial systems within their allocated resources. Due to the possibility that CHD could flow through the Microsoft Azure managed infrastructure and cloud environment Microsoft is seeking PCI DSS validation.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Microsoft Azure offers their customers IaaS and PaaS solutions, which their customers may use to store, process, or transmit CHD. As a business Microsoft Azure does not store, process, or transmit cardholder data (CHD).

Part 2c. Locations

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

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Data Center	64	Microsoft Azure uses facilities located around the world. The number listed after each location indicates the number of centers in each geographic location. **North America** 1. Northlake, IL (2) 2. San Antonio, TX (4) 3. Santa Clara, CA (4) 4. West Des Moines, IA (4) 5. Bristow, VA (1) 6. Boydton, VA (4) 7. Ashburn, VA (3) 8. Reston, VA (1) 9. Redmond, WA (1)

10. Quebec City, Quebec, Canada (1)
11. West Toronto, Ontario, Canada (1)
12. Humacao, Puerto Rico (1)
13. Cheyenne, WY (2)
14. Quincy, WA (2)
15. Tukwila, WA (1)

Europe

1. Dublin, Ireland (5)
2. Amsterdam, Netherlands (1)
3. Vienna, Austria (1)
4. Vantaa, Finland (1)
5. Frankfurt, Germany (1)
6. Biere, Germany (1)
7. Bettermbourg, Luxembourg (1)
8. Schiphol-Rijk, Netherlands (3)
9. Middenmeer, Netherlands (1)

Asia

1. Hong Kong, China (2)
2. Singapore (3)
3. Ambattur, India (1)
4. Mumbai, India (1)
5. Dighi, India (1)
6. Osaka, Japan (2)
7. Saitama, Japan (1)
8. Tokyo, Japan (1)

South America

1. São Paulo, Brazil (3)

Australia

1. Melbourne (1)
2. Macquarie (1)

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)
Not Applicable	N/A	N/A	N/A	N/A

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).*	Microsoft Azure is a cloud service provider, offering hardware, infrastructure, and computing platforms for building, deploying, and managing applications and services. Microsoft Azure does this through a global network of Microsoft Corporation and third-party managed datacenters. Microsoft Azure supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings. Microsoft

- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Azure product offerings are designed to meet their customers' security, privacy, and compliance requirements. Microsoft Azure physical infrastructure is owned and managed by Microsoft Cloud Infrastructure and Operations (MCIO).

Microsoft Azure doesn't directly store, process, or transmit card holder data (CHD); however, their tenant customers have the ability to operate ecommerce, and financial systems within their allocated resources. Due to the possibility that CHD could flow through the Microsoft Azure managed infrastructure and cloud environment Microsoft is seeking PCI DSS validation.

Microsoft Azure offers their customers IaaS and PaaS solutions, which their customers may use to store, process, or transmit CHD. As a business, Microsoft Azure does not store, process, or transmit cardholder data (CHD). Microsoft Azure customers are responsible for the security of the CHD they store, process, or transmit. The Microsoft Azure environment was assessed with the assumption all data was CHD.

Microsoft Azure does not store, process, or transmit CHD as part of their business model. Microsoft Azure does not have any payment channels.

Cardholder Data Environment:

Technical staff:

- Architects who design services, systems and networks
- Network engineers who build, test and support operations
- System engineers who build, test and support operations
- Security engineers who design, implement and monitor key systems and infrastructure via vulnerability management systems and log monitoring and alerting
- Software developers, who test and support operations
- Database administrators who support storage and data services

Management staff:

- Management with oversight of service development and operations
- Compliance specialists with oversight and management, including PCI
- Product developers of Microsoft PilotFish service offerings
- Project Managers who coordinate between service teams and support project management

- Service architects supporting client implementations and build outs

Business staff:

- Executives with oversight and guidance for PCI and business operations
- Back office specialists who support, billing and accounting functions

HR staff who perform background checks, personnel skills development operations, and training for existing staff

Technology Functions:

- Secure Software Development Lifecycle
- Development and maintenance of security and configuration standards
- System and network device maintenance and patching
- Maintaining approved configurations and correcting deviations
- Auditing and monitoring of in-scope systems and network devices
- Cryptographic Key Management supporting services reliant on unique secrets and services implementing encryption
- Database management and maintenance for internal and client-facing services
- Change Management for tracking and approving all changes
- Log monitoring and alerting as part of Vulnerability Management, supporting anti-malware, IDS, FIM, scanning and pen testing processes
- Vulnerability Management via internal and external scanning and penetration testing
- Identity Management via Active Directory and RAMweb

Business Functions:

- Information Risk Management
- Incident Response
- Billing and client onboarding processes

HR supporting staff vetting, onboarding, development and secure separation

Technologies:

Operating Systems: including Windows server and client versions

	Virtualization: custom hypervisors to manage resources and enhance isolation of multi-tenant client environments and realize efficiencies
	Databases: multiple vendors and versions, supporting service implementations and as services themselves
	Web portals for client and service management
	Encryption: custom implementations, including HSM
	VPN: enabling remote access for administrative work and client access
	Network devices: routers, switches architected in a tiered design to enhance management and isolation of CDE traffic.
	Firewalls: filter traffic to/from the CDE and between the client and management networks
	Anti-malware: both industry solutions and custom endpoint protection for service and client servers
	Vulnerability scanning, both internal and external, both service-focused and on client resources
	Change management software to track and record approval of infrastructure and software changes.
	Secret Store: Secure, encrypted storage for Microsoft PilotFish and customer secrets and encryption keys.

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:
Not Applicable	Not Applicable

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: Microsoft Azure

	Details of Requirements Assessed			
PCI DSS Requirement	**Full**	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	Requirements 1.2.3, 1.3.7, and 1.4 were deemed Not Applicable since wireless networks do not exist in the Microsoft C&E environment.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 was deemed Not Applicable since wireless networks do not exist in the Microsoft C&E environment. Requirement 2.2.3 was deemed Not Applicable since POS terminals do not exist in the Microsoft C&E environment.
Requirement 3:	☐	☒	☐	Requirement 3.2 was deemed Not Applicable as Microsoft C&E does not knowingly store, process, or transmit sensitive authentication data and thus treats all customer data as if it were cardholder data. Requirements 3.2.1-3.2.3 and 3.3 were deemed Not Tested as all customer data is encrypted at all times and Microsoft C&E staff do not have access to the keys needed to decrypt customer data and verify the potential presence of CHD.

				Requirements 3.6 and 3.6.6 were deemed Not Applicable since Microsoft C&E encryption keys never exist in cleartext and Microsoft C&E does not handle customer encryption keys.
Requirement 4:	☐	☒	☐	Requirements 4.1.1 and 4.2 were deemed Not Applicable since wireless networks do not exist in the Microsoft C&E environment and customer data is not allowes to be sent through end-user messaging technologies.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Requirements 6.5.7-6.5.10 and 6.6 were deemed Not Applicable since there are no web applications in the Microsoft C&E environment.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Requirement 8.1.5 was deemed Not Applicable since Microsoft C&E does not allow vendors to access system components within their CDE.
				Requirements 8.1.6.b, 8.2.1.d, 8.2.1.e, 8.2.4.b, and 8.2.5.b were deemed Not Applicable since Microsoft C&E does not handle password policies for their customers.
				Requirement 8.7 was deemed Not Tested as all customer data is encrypted at all times and Microsoft C&E staff do not set policies for customer databases.
Requirement 9:	☐	☒	☐	Requirement 9.8.1 was deemed Not Applicable since hard copies of customer data does not exist in the Microsoft C&E environment.
				Requirements 9.9-9.9.3 were deemed Not Applicable since POS terminals do not exist in the Microsoft C&E environment.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Requirement 11.1.1 was deemed Not Applicable since wireless networks do not exist in the Microsoft C&E environment.
Requirement 12:	☒	☐	☐	
Appendix A:	☐	☐	☒	Microsoft C&E is not a shared hosting provider.

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:	*June 30, 2016*	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☒ Yes	☐ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *June 30, 2016*, 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 *March 4, 2016*: ***(check one):***

☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Microsoft Cloud & Enterprise* has demonstrated full compliance with the PCI DSS.

☐ **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 *Microsoft Cloud & Enterprise* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance: N/A

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

☐ **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.

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met
N/A	N/A
N/A	N/A

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.1*, and was completed according to the instructions therein.

☒ All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.

☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☒ 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)

☒ 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.

☒ ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys*

Part 3b. Service Provider Attestation

Alice Rison

Signature of Service Provider Executive Officer ↑ | *Date:* **June 30, 2016**

Service Provider Executive Officer Name: **Alice Rison** | *Title:* **Principal Group PM Manager**

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed: | *QSA reviewed documentation, conducted interviews on-site, and confirmed accuracy of network architecture.*

Deepa Saldanha

Signature of Duly Authorized Officer of QSA Company ↑ | *Date:* **June 30, 2016**

Duly Authorized Officer Name: **Deepa Saldanha** | *QSA Company:* **Coalfire Systems, Inc.**

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed: | *Not Applicable*

Not Applicable

Signature of ISA ↑ | *Date: Not Applicable*

ISA Name: Not Applicable | *Title: Not Applicable*

[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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	