



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments - Service Providers

Version 3.2

April 2016



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:	Flexential	DBA (doing business as):	Not Applicable		
Contact Name:	David Kidd	Title:	Vice President of Governance Risk and Compliance		
Telephone:	+1 (704) 264-1025	E-mail:	david.kidd@peak10.com		
Business Address:	Plaza Tower One, 6400 S Fiddlers Green Cir #2000	City:	Greenwood Village		
State/Province:	Colorado	Country:	United States of America	Zip:	80111
URL:	https://www.flexential.com/				

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

Company Name:	A-LIGN				
Lead QSA Contact Name:	Patrick Ibrahim	Title:	Senior Consultant		
Telephone:	+1 (888) 702-5446	E-mail:	Patrick.Ibrahim@A-LIGN.com		
Business Address:	400 N. Ashley Drive Suite 1325	City:	Tampa		
State/Province:	Florida	Country:	United States of America	Zip:	33602
URL:	www.A-LIGN.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: Flexential Managed Compliant Cloud, Flexential Client Center Cloud

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):
Compliant Cloud Hosting

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): Not Applicable

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.



Part 2a. Scope Verification (continued)

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: Individual Managed Services, Non-compliant Public and Private Cloud, Colocation Services, Professional Services

Type of service(s) not assessed:

<p>Hosting Provider:</p> <input type="checkbox"/> Applications / software <input checked="" type="checkbox"/> Hardware <input checked="" type="checkbox"/> Infrastructure / Network <input checked="" type="checkbox"/> Physical space (co-location) <input checked="" type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input checked="" type="checkbox"/> Other Hosting (specify): Non-compliant Cloud Hosting	<p>Managed Services (specify):</p> <input checked="" type="checkbox"/> Systems security services <input checked="" type="checkbox"/> IT support <input checked="" type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<p>Payment Processing:</p> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management <input type="checkbox"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/>	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services <input type="checkbox"/>	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments <input type="checkbox"/>

Others (specify): Professional Services

Provide a brief explanation why any checked services were not included in the assessment:	The purpose of this assessment was to only evaluate Flexential's Managed Compliant Cloud and Client Center Cloud services. All other services were outside the scope of this assessment. Some Flexential services, such as colocation, are assessed separately for PCI compliance.
---	--



Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Flexential's Managed Compliant Cloud and Client Center Cloud environments do not store, process, or transmit CHD. Flexential provides IaaS, security services, disaster recovery and cloud-hosting services to its customers, however, no CHD is handled, stored or processed by Flexential on behalf of their customers.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Flexential focuses on protection and management of virtual and physical systems. Furthermore, Flexential provides administrative, technical and physical security controls to adequately protect infrastructure and system components within the cloud-hosting and IaaS environments. No CHD is handled, stored or processed by Flexential on behalf of their customers.

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Corporate Headquarters	1	Charlotte, NC
Datacenter	12	<ul style="list-style-type: none"> • Allentown data center - Allentown, PA • Aurora data center - Denver, CO • Centennial data center - Denver, CO • Richardson data center - Richardson, TX • Downtown Salt Lake City data center - Salt Lake City, UT • Calgary data center - Calgary, Canada • Brookwood data center - Brookwood, OR • AMS - Amsterdam, The Netherlands • ASH - Ashburn, VA • KC - Kansas City, MO • NL - Amsterdam, The Netherlands • SEA - Seattle, WA



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.	Not Applicable.	Not Applicable.	<input type="checkbox"/> Yes <input type="checkbox"/> No	Not Applicable.

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.*

The scope of the assessment was limited to the Flexential physical data centers where the Managed Compliance and Client Center Cloud environments resides, along with the infrastructure and security services residing in these environments, the client firewall services, and the security services supporting clients. The Flexential managed security services includes the provisioning of new systems, firewall management, initial configuration management, patching, vulnerability scanning, file integrity monitoring, log management, and antivirus.

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 a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

Yes No

If Yes:

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), 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:

Name of service provider:

Description of services provided:

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:		Flexential Managed Compliant Cloud, Flexential Client Center Cloud		
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"/>	1.3.6 - No system components store cardholder data.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - No wireless systems exist within Flexential’s environment. 2.2.3 - No insecure services, protocols or daemons are in use. 2.6 - Flexential is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Flexential does not store, process or transmit cardholder data.
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Flexential does not store, process or transmit cardholder data.
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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 - No third-party accounts exist within Flexential’s environment. 8.5.1 - No POS or Payment Capture devices exist within Flexential’s environment. 8.7 - Flexential does not have any Databases that store CHD.



Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.1.2 - No publicly accessible network jacks were present in Flexential's environment.</p> <p>9.6.2 - Flexential does not distribute any media to external entities or individuals at any time.</p> <p>9.6.3 - Flexential does not distribute any media to external entities or individuals at any time, nor is media moved from secure locations.</p> <p>9.8.1 - Flexential does not store any hard-copy materials containing sensitive data.</p> <p>9.8.2 - Flexential does not store any hard-copy materials containing sensitive data.</p> <p>9.9 - Flexential does not have any POS or payment capture devices in their environment.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.2.1 - Flexential does not store, process or transmit CHD.
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Flexential is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Flexential does not utilize early SSL or TLS.

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:	April 20 th , 2018
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 type="checkbox"/> Yes <input checked="" 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

This AOC is based on results noted in the ROC dated April 20th, 2018.

Based on the results documented in the ROC noted above, 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 (**check one**):

<input checked="" type="checkbox"/>	Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Flexential</i> has demonstrated full compliance with the PCI DSS.						
<input type="checkbox"/>	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. Target Date for Compliance: 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>						
<input type="checkbox"/>	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. <i>If</i>						
	<table border="1"> <thead> <tr> <th>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</i> , Version 3.2, 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

DocuSigned by:



5B0CB752B79A479...

Signature of Service Provider Executive Officer 

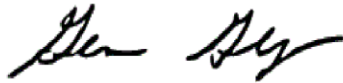

Date: 4/20/2018

Service Provider Executive Officer Name: David Kidd

Title: Vice President of GRC

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

The assessor provided PCI DSS advisory and assessment services, which included onsite observation of controls, interviews with key personnel, and review of policies and procedures.Signature of Duly Authorized Officer of QSA Company 

Date: 4/20/2018

Duly Authorized Officer Name: Gene Geiger, President

QSA Company: A-LIGN

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

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	<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 type="checkbox"/>	<input type="checkbox"/>	Not Applicable.
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	Not Applicable.
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"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input type="checkbox"/>	<input type="checkbox"/>	Not Applicable.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	<input type="checkbox"/>	<input type="checkbox"/>	Not Applicable.

