Requisitos Básicos de Validación del Programa de Seguridad de Información (AIS – PCI DSS)

February 14, 2019

Raimundo Villar – Risk Analyst, Ecosystem Data Security

VISA

Avisos Legales

"Como Está": Resultados de encuestas, investigaciones y recomendaciones de mejores prácticas se proporcionan "COMO ESTÁ", sol amente para fines informativos y no deberán ser consideradas como asesoría comercial, legal, regulatoria, fiscal, financiera o de otro tipo. Recomendaciones de mejores prácticas o materiales deben evaluarse por separado en base a sus propias necesidades comerciales específicas y en vista de las leyes y normativas que aplican a su situación particular. Visa no es responsable por el uso que usted pueda hacer de los resultados de encuestas, investigaciones o recomendaciones de mejores prácticas ni de ninguna otra información, incluidos errores de cualquier tipo, ni por cualquier presunción o conclusión que usted pudiera inferir del uso de los mismos.

Mejores Prácticas: La información, recomendaciones o "mejores prácticas" contenidas en este documento se proporcionan COMO ES TÁ", solamente exclusivamente para fines informativos, y no deberán considerarse como asesoría de negocios, de mercadeo, operativa, comercial, financiera, legal, técnica, fiscal o de otro tipo. Materiales de mercadeo recomendadas deberán ser evaluadas independientemente a la luz de sus necesidades comerciales y las leyes y regulaciones aplicables. Visa no se hace responsable por su uso de materiales de mercadeo, recomendaciones de mejores prácticas, u otra información, incluyendo errores de ningún tipo, contenidas en este documento.

Productos/Ideas en Desarrollo: Este documento es solamente para fines ilustrativos. Contiene descripciones de producto(s) act ualmente en proceso de implementación, y debe entenderse como una representación de las características potenciales de los producto(s) al estar completamente desplegadas. La versión final de los producto(s) puede no contener todas las características descritas en esta presentación.

Confidencialidad: Este documento se le proporciona exclusivamente basado en su carácter de cliente de Visa o miembro del sist ema de pagos de Visa. Al aceptar este documento, usted reconoce que la información aquí contenida (la "Información") es confidencial y está sujeta a restricciones de confidencialidad contenidas en el reglamento operativo de Visa y otros acuerdos de confidencialidad, que limitan el uso que usted puede hacer de la Información. Usted accede a mantener la Información como confidencial y no utilizarla para cualquier otro propósito distinto de aquél que le compete en su carácter como cliente de Visa Inc. o como miembro del sistema de pagos de Visa. La Información solo podrá ser diseminada dentro de su organización según sea necesario para fin de permitir su continuada participación en el sistema de pagos de Visa. Se le notifica que la Información podría constituir información sustancial no pública conforme a las leyes federales de títulos-valores de EE.UU. y que la compraventa de títulos-valores de Visa estando usted al tanto de información substancial la cual que no es de conocimiento publico podría constituir una violación a las leyes federales de títulos-valores de EE.UU. que pudieran aplicar.

Declaraciones a futuro: Esta presentación podría contener declaraciones a futuro según se definen en la ley de Estados Unidos conocida como el Private Securities Litigation Reform Act de 1995. Estas declaraciones se pueden identificar por los términos "esperar", "será", "continuar" y referencias similares al futuro. Por su naturaleza, las declaraciones a futuro: (i) se refieren únicamente a la fecha en que son realizadas; (ii) no son declaraciones de hechos históricos ni garantía sobre desempeño futuro; y (iii) se encuentran sujetas a riesgos, incertidumbre, suposiciones y cambio de circunstancias que difícilmente se pueden predecir o cuantificar. Visa describe en sus notificaciones registradas con la SEC los riesgos e incertidumbres que pudieran dar lugar a que los resultados finales difieran de manera importante o se opongan a declaraciones a futuro. A menos que la ley lo requiera, Visa no tiene intención de actualizar o revisar cualquier declaraciones a futuro aquí contenida en virtud de nueva información, eventos futuros o por cualquier otra razón.

Agenda

1. Panorama de amenazas y la Estrategia de Seguridad de Visa
2. Entendiendo el Cumplimiento y Validación de los Requisitos de PCI DSS
3. Errores Comunes de Documentación de Validación
4. Utilizando el Enfoque Priorizado
5. Recursos de seguridad de datos
6. Preguntas

Panorama de Amenazas

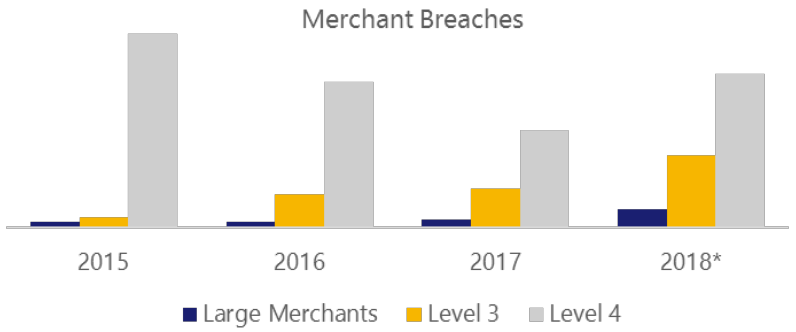
Tendencias Globales de Compromiso

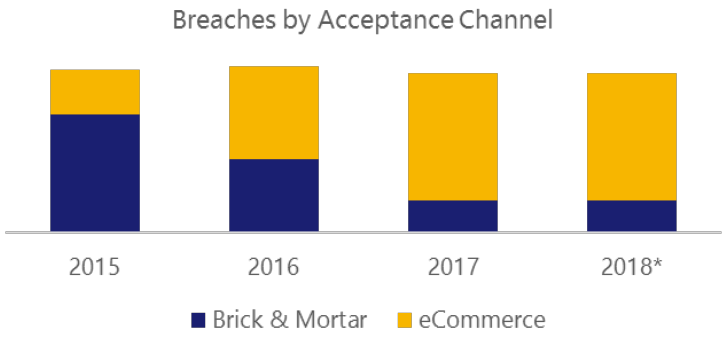
Cambios en Tipos de Violaciones

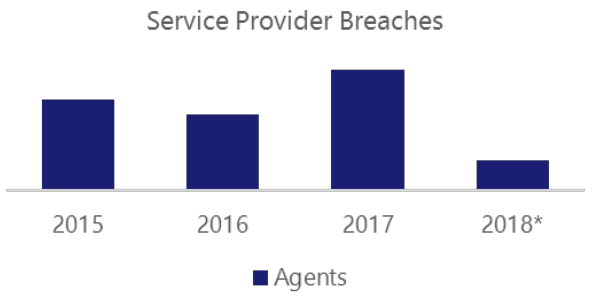
- Disminución de los eventos que involucran datos de banda magnética
- Aumento de los compromisos de eCommerce.
- Proliferación de violaciones de terceros.

Criminales moviéndose más allá de los comerciantes

- Enfocando en agregadores e integradores / revendedores de datos
- Creciente interés en los proveedores de servicios de comercio electrónico
- Penetrando las instituciones financieras







Estrategia de Seguridad de Visa

Los Datos son Clave para Abordar las Amenazas

Proteger Datos

Resguardar los Datos de Pago

Utilizar Datos

Detener el fraude antes de que ocurra

Devaluar datos

Hacer datos inútiles

Habilitar a los Consumidores

Involucrar a los Tarjetahabientes en la Seguridad de Pago

Programa de Seguridad de Información de Cuentas (AIS) de Visa

Protección de la información de cuentas es crítico

¿Qué es el Programa AIS Visa?

- Programa de cumplimiento global centrado en la protección de la información de la cuenta Visa en todo el ecosistema de pagos.
- Establece requisitos para el cumplimiento y la validación de los estándares de seguridad de la industria para clientes de Visa, comerciantes, procesadores, agentes terceros y otras partes interesadas de la industria.

¿Cuáles son los objetivos del programa?

- Mantener la seguridad e integridad del ecosistema de pagos de Visa.
- Proactivamente defenderse de los compromisos de datos de cuentas Visa a través del monitoreo del cumplimiento con PCI DSS y resolver las deficiencias de seguridad identificadas.
- Incentivar la adopción de tecnologías y prácticas seguras de aceptación.

PCI DSS: Entender el Cumplimiento y la Validación

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)

Cumplimiento + Validación

Cumplimiento

- Visa requiere que **TODAS** las organizaciones que almacenen, transmitan o procesen datos de cuentas Visa tienen que cumplir con los estándares PCI DSS.
- PCI DSS se aplica a todos los canales de pago, incluida la tarjeta presente, el pedido por correo o teléfono, el comercio electrónico, la aplicación, etc.

Validación

- Separada y distinta del requisito de cumplir con PCI DSS es la validación de cumplimiento.
- La validación es el ejercicio de verificar y demostrar el estado de cumplimiento con los requisitos de los estándares PCI DSS.

Funciones y Responsabilidades de los Interesados

Visa	Clientes	Comercios y Proveedores de Servicios	PCI SSC
▪ Establecer y hacer cumplir los programas de cumplimiento para garantizar que las partes interesadas protejan los datos de acuerdo con los estándares de la industria ▪ Proporcionar educación de seguridad de datos y conciencia sobre amenazas y estrategias de mitigación ▪ Promover el uso de tecnologías de aceptación seguras	▪ Asegurar que los comercios y agentes patrocinados que manejan los datos de cuenta en su nombre cumplan con PCI DSS ▪ Proporcionar actualizaciones de estatus a Visa de acuerdo con el Programa AIS	▪ Proteja los datos de cuentas Visa de acuerdo con los estándares PCI DSS y otras normas de seguridad de datos aplicables ▪ Validar el cumplimiento con PCI DSS según lo requerido por el programa AIS de Visa	▪ Desarrollar y gestionar los estándares PCI DSS, herramientas de validación, documentación de orientación y apoyo material educativo ▪ Capacitar y administrar evaluadores de seguridad calificados, proveedores de escaneo aprobados, integradores y revendedores calificados, y otros programas de certificación

Documentación de validación de PCI DSS

Informe de Cumplimiento (ROC)

- Informe que documenta los resultados detallados de la evaluación de la entidad frente a cada requisito individual de los estándares PCI DSS.
- La plantilla incluye un resumen completo del entorno de la entidad (Secciones 1 a 5), campos para las descripciones individuales de los requisitos de PCI DSS, procedimientos de prueba, instrucciones de informe y respuestas del asesor.
- El informe también incluye apéndices complementarios que pueden ser aplicables para ciertas entidades.

Cuestionario de Autoevaluación (SAQ)

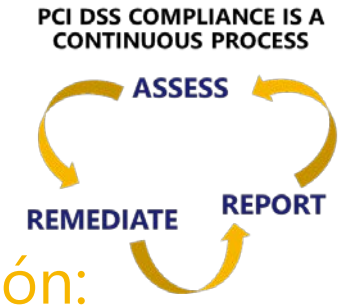
- Herramienta de informes utilizada para documentar los resultados de la autoevaluación de los requisitos de PCI DSS de la entidad.
- Cuestionario con una serie de preguntas de “SÍ o NO” para cada requisito de PCI DSS aplicable
- Hay 9 cuestionarios diferentes disponibles para satisfacer diferentes entornos de aceptación

Atestación de Cumplimiento (AOC)

- Formulario para que los comerciantes y proveedores de servicios certifiquen los resultados de la evaluación de PCI DSS, como se documenta en el ROC o SAQ.

VISA

Proceso de Validación de PCI DSS



Evaluación de Cumplimiento y Pasos para Validación:

1. Alcance – Determine qué componentes del sistema y redes están dentro del alcance de las PCI DSS
2. Evaluar – Examine el cumplimiento de los componentes del sistema en el alcance siguiendo el procedimiento de prueba para cada requisito de PCI DSS
3. Remediar – Si es necesario, realice una corrección para abordar los requisitos que no están implementados y proporcione un informe actualizado
4. Informar – El evaluador y / o la entidad completan la documentación de validación requerida (por ejemplo, SAQ o ROC), incluida la documentación de todos los controles de compensación
5. Atestiguar – Complete la Atestación de Cumplimiento (AOC) apropiada
6. Enviar – Presente el SAQ, ROC, AOC y otra documentación de respaldo al adquirente o Visa según sea necesario

Source: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1536263962218

Requisitos de Validación PCI DSS de Visa

Comercios

Nivel	Volumen Anual de Transacciones	Requisitos Mínimos de Validación
1	6 millones + transacciones Visas (todos los canales)	• Informe de Cumplimiento (ROC) por parte del Asesor de Seguridad Calificado (QSA) o (ISA) o recursos internos si está firmado por un director de la compañía • Atestación de Cumplimiento (AOC)
2	1 millón a 6 millones de transacciones Visa (todos los canales)	• Cuestionario de Autoevaluación (SAQ) • Atestación de Cumplimiento (AOC)
3	20.000 a 999.999 transacciones Visa en comercio electrónico	• Cuestionario de Autoevaluación (SAQ) • Atestación de Cumplimiento (AOC)
4	Menos de 20,000 transacciones Visa en comercio electrónico y todos los demás comerciantes que procesan menos de 1 millón de transacciones Visa	• Cuestionario de autoevaluación (SAQ) o validación alternativa según lo definido por el adquirente

Proveedores de Servicios

Nivel	Volumen Anual de transacciones	Requisitos Mínimos de Validación
1	More than 300,000 Visa transactions	• Informe de Cumplimiento (ROC) por un Asesor de Seguridad Calificado (QSA) • Atestación de Cumplimiento (AOC)
2	Less than 300,000 Visa transactions	• Cuestionario de Autoevaluación (SAQ)* • Atestación de Cumplimiento (AOC)

* Los proveedores de servicios deben completar una ROC completa utilizando un PCI QSA para ser incluidos en el Registro Global de Proveedores de Servicios de Visa, sin importar el nivel.

Errores Comunes en Documentación de Validación

Atestación de Cumplimiento

¿Todos los canales de aceptación de pagos están identificados y evaluados?

Section 1: Assessment Information

Instructions for Submission

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

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	Geti Gas Station		DBA (doing business as):	Geti Gas Station	
Contact Name:	Rai Villar		Title:	Owner	
Telephone:	305-639-2354		E-mail:	rai@getigas.com	
Business Address:	123 Main Street		City:	Miami	
State/Province:	FL	Country:	USA	Zip:	33125
URL:	www.getigas.com				

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

Company Name:	QSA Secure your Network				
Lead QSA Contact Name:	John Secure		Title:	Senior Consultant	
Telephone:	786-214-9865		E-mail:	john@qsasecure.com	
Business Address:	654 Back Street		City:	Princeton	
State/Province:	FL	Country:	USA	Zip:	33658
URL:	www.qsasecure.com				

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☒ Petroleum	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ Others (please specify):		

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
☐ Mail order/telephone order (MOTO)	☐ ~~Mail order/telephone order (MOTO)~~
☒ E-Commerce	☐ E-Commerce
☒ Card-present (face-to-face)	☒ Card-present (face-to-face)

***Note:** If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.*

Descripciones comúnmente olvidadas. . .

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	Geti Gas Stations accept payments card at the gas pump terminals, POS and by a smartphone application.

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)
Example: Retail outlets	*3*	*Boston, MA, USA*
Retail outlets	10	Miami, FL, USA

Part 2d. Payment Application

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)
Getpaid now	1.5	Getpaid Now, LLC	☐ Yes ☒ No	
Advance Checkout Solution (ACS)	6.2.7.x	NCR	☒ Yes ☐ No	Oct. 22, 2022
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	All conneciton in and out of the CDE. All POS, terminals and all necessary payments components are included in this assessment.

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	☒ Yes ☐ No
If Yes:	
Name of QIR Company:	POS Sales and Instalations
QIR Individual Name:	Bob POS
Description of services provided by QIR:	POS Sales, instalation and technal support
Does your company share cardholder data with any 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.)?	☒ Yes ☐ No
If Yes:	
Name of service provider:	**Description of services provided:**
Dolphins Payment Gateway	Payment Gateway
Badu payment processors	payment processessing.

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

Revise esas casillas. . .

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:	08/20/2018	
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

This AOC is based on results noted in the ROC dated *(ROC completion date).*

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):***

☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Geti Gas Stations 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 *(Merchant Company Name)* 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. *Check with your acquirer or 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

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 v3.2.1, 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.

VISA

¡Las firmas y fechas son importantes!

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 True Link, INC.

Part 3b. Merchant Attestation

P. Villar

Signature of Merchant Executive Officer ↑	*Date:* **8/20/2018**
Merchant Executive Officer Name: **Rai Villar**	*Title:* **CEO**

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

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

John

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 8/20/2018
Duly Authorized Officer Name: John Secure	*QSA Company:* QSA Secure your Network

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:	N/A

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 your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One) YES	NO	Remediation Date and Actions (If "NO" selected for any Requirement)
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	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	

PCI DSS y el Enfoque Priorizado

Priorizar el Enfoque de Conformidad con PCI DSS

Reducir el Riesgo Temprano en el Proceso de Cumplimiento

Enfoque priorizado de PCI SSC 

- Proporciona seis hitos de seguridad para ayudar a las organizaciones a protegerse de manera incremental contra los factores de mayor riesgo mientras trabajan para el cumplimiento de PCI DSS
- Sirve como una ruta para priorizar la implementación de controles de seguridad
- Apoya la planificación financiera y operativa
- Promueve indicadores de progreso objetivos y medibles

Recordatorios! 

- El Enfoque Priorizado no es un sustituto, atajo o interrupción de brechas para el cumplimiento de PCI DSS
- No es obligatorio ni conveniente que todas las organizaciones utilicen o sigan el Enfoque priorizado
- Para lograr el cumplimiento de PCI DSS, las organizaciones deben cumplir con todos los requisitos de PCI DSS, independientemente del orden en que se implementen

VISA

Asegúrese de que el Plan esté Completo

PCI DSS Requirements v3.2.1	Milestone	Status *Please enter "yes" if fully compliant with the requirement*	If status is "N/A", please explain why requirement is Not Applicable	If status is "No", please complete the following		
				Stage of Implementation	Estimated Date for Completion of Milestone	Comments
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	Yes				
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1	N/A	No Wireless Networks			
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1	No		Planning	October 15, 2018	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2	Yes				
1.1.5 Description of groups, roles, and responsibilities for management of network components	6	No		Implementation In Progress	October 15, 2018	
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2	No		Implemented But Not Validated	October 30, 2018	
1.1.7 Requirement to review firewall and router rule sets at least every six months	6	Yes				
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2	Yes				
1.2.2 Secure and synchronize router configuration files.	2	Yes				
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	2	No		Implementation In Progress	November 30, 2018	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	2	Yes				
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	2	No		Planning	November 30, 2018	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	2	No		Planning	November 30, 2018	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	2	Yes				
1.3.5 Permit only "established" connections into the network.	2	No		Planning	November 30, 2018	

VISA

Fechas Hito de Finalización

Revisar y Reconocer los Objetivos de Finalización Razonables

Prioritized Approach Summary & Attestation of Compliance*

Milestone	Goals	Percent Complete	Estimated Date for Completion of Milestone
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it	88.9%	October 15, 2018
2	**Protect systems and networks, and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises, and the processes for responding.	94.1%	November 30, 2018
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.	100.0%	
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.	100.0%	
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.	100.0%	
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.	97.1%	October 15, 2018
Overall		97.1%	**November 30, 2018**

An entity submitting this form may be required to complete an Action Plan. Check with your acquirer or the payment brand(s) since not all payment brands require this section.

Part 5: Target Date for Achieving Full PCI DSS Compliance — Date: 30-Nov-18

Part 6: Merchant or Service Provider Acknowledgements

Signature of Executive Officer: **Bruce Joe** — Date: 1-Sep-18

Considere Oportunidades de Reducción de Alcance

Less Data = Less Risk

Cifrado Punto a Punto (P2PE)

- Implemente una solución P2PE validada por PCI para cifrar los datos de la cuenta a lo largo del ciclo de vida de la transacción, sin que sea posible descifrarla en el entorno del comerciante

Segmentación de la red

- Establezca un marco de red que utilice herramientas y procesos seguros para aislar el entorno de datos de la cuenta del resto de la red

Subcontratación

- Subcontratar la aceptación de pagos y el procesamiento de datos a un proveedor de servicios validado por PCI incluido en el Registro Global de Proveedores de Servicios de Visa

EMVCo Tokenización

- Comience a aceptar los tokens de pago generados de acuerdo con la Especificación de Tokenización de EMVCo para eliminar datos confidenciales de cuentas

VISA

Recursos de Seguridad de Datos

Recursos de Seguridad de Datos

Visa Data Security Website www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers, Webinars

Visa Global Registry of Service Providers www.visa.com/onthelist

- List of registered, PCI DSS validated third party agents

PCI Security Standards Council Website www.pcissc.org

- Data Security Standards, Qualified Assessor Listings, Data Security Education Materials

PCI Resources for Small Merchants
https://www.pcisecuritystandards.org/merchants/

- Guide to Safe Payments, Common Payment Systems, Questions to Ask your Vendors
- Payment Data Security Essentials: Video and Infographics

VISA

Visa's Ecosystem Data Security Team

Questions? Comments?

- Agent Registration: Agents@visa.com
- Third Party Compliance: pciagents@visa.com
- Merchant Compliance: cisp@visa.com
- AVP: vendorcompliance@visa.com
- 3DS Security: acs@visa.com
- PIN security: pinsec@visa.com

Preguntas

¡Gracias!