



Account Information System (AIS) Program

Frequently Asked Questions

Q What is AIS?

A Account Information Security, or AIS, is a Risk Management program by Visa aimed to protect account and/or transaction information whereby all entities which process, store, and/or transmit account and transaction information must be compliant with the Payment Card Industry (PCI) Data Security Standards (DSS).

The five major card brands founded the PCI Security Standards Council (PCI SSC) in 2006 to oversee the standards itself, but each of the card brands maintain their own program that outlines the validation requirements, deadlines and fines.

To learn more about the PCI DSS and the PCI SSC, please visit the PCI SSC website at www.pcisecuritystandards.org.

Q Who is required to comply with the PCI DSS?

A All entities that store, process, or/and transmit cardholder data, such as merchants, service providers (e.g. payment gateways, IPSP, processors), issuers and acquirers, must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and mortar), mail/telephone order (MOTO) and e-commerce.

Q What if I outsource the handling, transmission or storage of cardholder data to a third party organization?

A Both issuing and acquiring banks must use, and are responsible for ensuring that their merchants use, service providers that are compliant with the PCI Data Security Standards. Although there may not be a direct contractual relationship between merchant service providers and acquiring members, Visa acquirers are responsible for any liability that may occur as a result of non-compliance.

Q How do I validate PCI DSS compliance?

A Validation requirements for merchants and service providers are based on the average annual volume of cardholder data handled by the organization. Please refer to www.visa-asia.com/secured for the merchant and service provider levels and requirements.

Validation tools:

- Annual on-site PCI Data Security Assessment by a PCI SSC Qualified Security Assessor (QSA).
- Quarterly vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)
- Annual self-assessment using the PCI DSS Self-Assessment Questionnaire (SAQ)

For the list of QSAs and ASVs and SAQ, please go to www.pcisecuritystandards.org.



Q What is the PCI Self-Assessment Questionnaire (SAQ)?

A The PCI Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. You can download the SAQ from www.pcisecuritystandards.org/saq/instructions.shtml.

Q What is a Vulnerability Scan?

A A vulnerability scan is an automated remote scan that assesses your network from the internet to see if you have any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data.

Q Is PCI DSS compliance a one-time requirement?

A No. PCI DSS compliance is an ongoing process. While validation actions vary depending on the actual number of transactions an entity process annually, all merchants and service providers are required to comply with PCI DSS at all times.

Q Is there a deadline to be compliant?

A Yes. The deadlines are as follows:

Level 1 Merchants

- Elimination of prohibited data storage deadline is **September 30, 2009**.
- PCI DSS compliance deadline is **September 30, 2010**.

Level 2 Merchants

- Elimination of prohibited data storage deadline is **September 30, 2009**.

Service providers

- PCI DSS compliance deadline is **December 31, 2008**.

Q How are the merchant levels defined and what are the validation requirements?

A Separate from the mandate to comply with the PCI DSS is the validation of compliance, whereby Visa has prioritized and defined validation levels based on the volume of transactions, the potential risk and exposure introduced into the Visa system. Visa has established globally aligned merchant levels and validation requirements for annual PCI DSS compliance validation as follows:

Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as level 1 by any Visa region	<ul style="list-style-type: none"> ▪ Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”) ▪ Quarterly network scan by Approved Scan Vendor (“ASV”) ▪ Attestation of Compliance Form

Level / Tier	Merchant Criteria	Validation Requirements
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"> ▪ Annual Self-Assessment Questionnaire ("SAQ") ▪ Quarterly network scan by ASV ▪ Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"> ▪ Annual SAQ ▪ Quarterly network scan by ASV ▪ Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"> ▪ Annual SAQ recommended ▪ Quarterly network scan by ASV if applicable ▪ Compliance validation requirements set by acquirer

**All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ("DBA"). In cases where a merchant corporation has more than one DBA, clients must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, members will continue to consider the DBA's individual transaction volume to determine the validation level as follows.*

Q How are the service provider levels defined and what are the validation requirements?

A Visa has established globally aligned levels and validation requirements for annual PCI DSS compliance validation for service providers as follows:

Level	All Regions	Validation Requirements
1	VisaNet processors or any service provider that stores, processes and / or transmits over 300,000 transactions per year	<ul style="list-style-type: none"> • Annual ROC by QSA • Quarterly network scan by ASV • Attestation of Compliance Form
2	Any service provider that stores, processes and / or transmits less than 300,000 transactions per year	<ul style="list-style-type: none"> ▪ Annual SAQ ▪ Quarterly network scan by ASV ▪ Attestation of Compliance Form

Q What if I choose not to be involved in the AIS program?

A The AIS program is globally mandated for all Visa issuing and acquiring banks and their agents (e.g. merchants, service providers etc). Should an issuer's or acquirer's agent be found not compliant with the AIS requirements, the issuer or acquirer may be financially penalized by Visa. Ultimately, merchants and service providers must meet the AIS requirements to continue to accept Visa payment products.

Q. Who do I contact if I have questions about the AIS Program requirements?

A Please contact your acquiring bank, or visit the AIS website at www.visa-asia.com/secured.

For enquiries on the PCI DSS and its related information, please contact the PCI SSC at www.pcisecuritystandards.org/about/contact.shtml.

Payment Applications

Q What is PA DSS?

The Payment Application Data Security Standard (PA-DSS) is an industry standard, based on Visa's Payment Application Best Practices (PABP), originally created to support the PCI DSS and help software vendors and others develop secure payment applications that do not store prohibited data such as full magnetic stripe or other sensitive authentication data or PIN data. The PA-DSS is managed by the Payment Card Industry Security Standards Council (PCI SSC) along with other industry standards such as the PCI DSS and PCI PED, and is recognized by all major payment brands.

For more information on what is required to be PCI DSS-compliant, please visit www.pcisecuritystandards.org.

Q What types of payment applications are subject to the PA-DSS requirements?

A The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third-parties e.g. merchants, service providers.

Payment applications validated in accordance with PA-DSS, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe/track, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Q What types of payment applications are NOT subject to the PA-DSS requirements?

- A
1. Payment applications that are developed for and sold to only one customer are NOT subject to the PA-DSS requirements; however, they must be covered by the customer's PCI DSS assessment.
 2. Payment applications that are developed in-house by merchants or service providers and are not sold to a third party are NOT subject to PA-DSS, however, they must be covered by the merchants' or service providers' PCI DSS assessment.
 3. Payment applications that are resident in standalone point-of-sale terminals are NOT subject to the PA-DSS requirements
 4. The following list, while not all inclusive, illustrates applications that are NOT payment applications for purposes of PA-DSS: operating systems onto which a payment application is installed (for example, Windows, Unix), database systems that store cardholder data (for example, Oracle), and back-office systems that store cardholder data (for example, for reporting or customer service purposes).



Q Will the PCI SSC accept applications that have been previously validated under the existing Visa PABP program?

A PCI SSC will recognize PABP validated payment applications and list them with the appropriate PABP version that they were validated against. For further details, please refer to the table below.

		PCI SSC Listing Prior to Expiration		PCI SSC Listing After Expiration	
Version	Expiration Date	Validation Notes	Deployment Notes	Validation Notes	Deployment Notes
PABP 1.4	24 months	Validated according to PABP	Acceptable for new deployments	Validated according to PABP	Not acceptable for new deployments
PABP 1.3	18 months	Validated according to PABP	Acceptable for new deployments	Validated according to PABP	Not acceptable for new deployments
Prior to PABP 1.3	12 months	Pre-PCI application	Not recommended for new deployments	Pre-PCI application	Not acceptable for new deployments
PA-DSS 1.1	3 Years after change to standard	Validated according to PA-DSS	Acceptable for new deployments	Validated according to PA-DSS	Not acceptable for new deployments

Q How does the PA-DSS impact customers?

A Secure payment applications help to facilitate a customer's PCI DSS compliance. When implemented in a DSS-compliant environment, PA-DSS validated payment applications will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks.

Q Who will perform PA-DSS assessments?

A Only Payment Application Qualified Security Assessors (PA-QSA) accredited by the PCI SSC can perform payment application reviews.. Note that not all QSAs are PA-QSAs – there are additional qualification requirements that must be met for a QSA to become a PA-QSA. The list of PA-QSAs is published on the PCI SSC website.

Q How much does PA DSS validation cost?

A Compliance validation takes place at the software vendor's expense. The cost of PA-DSS validation is determined by a payment application's complexity and size, as well as the time required for review and PA-QSA pricing.