



VPSS Certification Frequently Asked Questions

What is the difference between Visa's Account Information Security (AIS) program and VPSS Certification?

The AIS program ensures compliance to the Payment Card Industry Data Security Standard (PCIDSS) standards with regards to the protection of cardholders' sensitive account and transaction information. Compliance to the AIS standards is a requirement for all entities participating in the Visa payment system.

VPSS Certification on the other hand is a review service that includes the examination of compliance to the AIS standards as well as other operational standards such as the Visa PIN Security standards, operations policy and procedures and data quality standards.

What is the cost of VPSS Certification?

Payment security controls, market conditions and business needs and activities vary widely among Visa members, service providers and merchants. To provide a more accurate pricing schedule, entities seeking for a review will be asked to submit a pre-engagement questionnaire that will provide Visa with information on scope and complexity of the review. Visa will however strive to provide quality service at the most competitive prices.



Why choose Visa for the review?

Visa Asia Pacific Risk management is intimately familiar with all *Visa International Operating Regulations* and associated standards.

As the world's leading payments brand and the largest payments system worldwide, Visa understands payment security best.

Visa's consultants are a group of experienced professionals who have the expertise and in-depth knowledge on all aspects of card payment.

Visa provides quality service at the most competitive prices.

Besides information security, we provide other aspects of review, including compliance to *Visa International Operating Regulations* and Operational Controls.

Visa provides additional benefits including the listing of certified entities and regular distribution of bulletins etc.

How do I justify the review cost?

As payment security threats continue to grow, a security review should be treated as an investment instead of a compliance cost. It is difficult to quantify the Return on Investment (ROI) for a review, as it has no direct addition to the bottom line. However, the cost of not doing the review is far greater. Just consider the consequences of a security breach:

- Financial losses
- Reputation damage
- Exposure to legal risks resulting from violating the privacy of cardholders.
- Loss of business opportunities as a result of lack of trust
- Impact of downtime resulting from attacks
- Potential payment scheme penalties / or termination of facility



After the initial review, why do I need subsequent reviews?

VPSS Certifications are valid for twelve months. The need for re-certification arises because security threats are constantly changing due to evolving technologies and new methods of attack. Security measures implemented today may be rendered obsolete in the next two years as a result of new technologies. Re-certification ensures the continued improvement of payment security standards and that the security measures are kept up-to-date.

What is the new PCI Data Security Standard?

The new Payment Card Industry (PCI) Data Security Standard outlines best practices for credit card data that is stored, processed or transmitted. It consolidates and supersedes the requirements of the previously developed MasterCard Site Data Protection (SDP) Program and the Visa AIS program. As such, the new standard contains IT security requirements and guidelines for all major credit card issuers, including Visa, MasterCard, American Express, Diners Club and Discover. These card issuers joined forces to develop the new requirements as part of an industry-wide standard for protection of cardholders' credit card account and transaction information.

When did the standard go into effect?

14 December 2004.

Are the VPSS Certification requirements for service providers aligned with other card brands?

The AIS standards and PIN Security Standards, which may be part of the review scope, are aligned with the industry wide Payment Card Industry Data Security Standard (PCIDSS) standards. Nevertheless, service providers and merchants are advised to contact other payment card companies directly to address concerns on the standards alignment.



Can a merchant/service provider be considered VPSS certified if they have outstanding non-compliance issues but provide a remediation plan?

Lack of full certification will prevent an entity from being considered VPSS Certified. Visa encourages entities to complete the initial review, develop a remediation plan; complete items on the remediation plan, and revalidate compliance of those outstanding items.

What if a merchant or service provider does not store Visa cardholder data?

If a merchant or service provider does not store cardholder data, VPSS Cert still applies to the environment that transmits or processes cardholder data.

When is it acceptable to store magnetic stripe data?

It is never acceptable for Acquirers, merchants, or service providers to retain magnetic stripe data subsequent to transaction authorization. The *Visa International Operating Regulations* prohibit storage of the contents of the magnetic stripe as a unit. The following individual data elements may be retained subsequent to transaction authorization:

- Cardholder Account Number
- Cardholder Name
- Card Expiration Date

When is it acceptable to store Card Verification Value 2 (CVV2)?

It is never acceptable for Acquirers, merchants, or service providers to retain CVV2, which consists of the last three digits printed on the signature panel of all Visa Cards, subsequent to transaction authorization. The *Visa International Operating Regulations* prohibit such storage, whether encrypted or unencrypted.



Are there alternatives, or compensating controls, that can be used to meet a requirement?

If a requirement is not, or cannot, be met exactly as stated, compensating controls can be considered as alternatives to requirements defined in AIS. Compensating controls should meet the intention and rigor of the original AIS requirement, and should also be examined by the assessor as part of the regular AIS audit. Compensating controls should be “above and beyond” other AIS requirements - it is not a compensating control to simply be in compliance with other AIS requirements.

Are there alternatives to encrypting stored data?

Stored cardholder data should be rendered unreadable according to requirement 3 of the PCI Security Audit Procedures document. If encryption, truncation, or another comparable approach cannot be used, encryption options should continue to be investigated as the technology is rapidly evolving. In the interim, while encryption solutions are being investigated, stored data must be strongly protected by compensating controls. These compensating controls should be considered as part of the compliance validation process.

An example of compensating controls for encryption of stored data is complex network segmentation that may include the following:

- Internal firewalls that specifically protect the database
- TCP wrappers or firewall on the database to specifically limit who can connect to the database
- Separation of the corporate internal network on a different network segment from production, fire-walled away from database servers.



What if a Member, merchant, or service provider has outsourced the storage, processing, or transmission of cardholder data to a service provider?

Members, merchants, and service providers should be in the process of positioning themselves to deal only with AIS-compliant service providers. If there are service providers handling cardholder data on an entity's behalf, the entity must ensure that contracts with these service providers specifically include AIS compliance as a condition of business. A list of compliant service providers can be found on the AIS Website.

Can a merchant/service provider be considered AIS compliant if they have outstanding non-compliance issues, but provide a remediation plan?

Lack of full compliance will prevent an entity from being considered AIS compliant (and receiving a VPSS Certification), however, Visa encourages entities to complete the initial review, develop a remediation plan, complete items on the remediation plan, and revalidate compliance of those outstanding items. For service providers, a Report On Compliance demonstrating full compliance must be provided to Visa prior to inclusion on the list of compliant service providers. Currently, there is not a comparable list for merchants.

Do merchants need to include their service providers in the scope of their review?

No. Service providers are responsible for validating their own compliance independent of their customers. Acquirers must identify service providers handling cardholder data on their merchant's behalf. Visa will then work with acquirers to ensure that these service providers validate compliance.