VISA EUROPE ACCOUNT INFORMATION SECURITY (AIS) PROGRAMME FREQUENTLY ASKED QUESTIONS (FAQS)

Q1: What is the purpose of the AIS programme?

A: The AIS programme aims to enhance the protection of sensitive account and transaction information in the Visa acceptance environment. It protects the interests of all payment participants, including Members, merchants and cardholders—in both the physical and virtual world. Visa was the first in the industry to create such a programme, including standards and self-assessment security tools.

Q2: What exactly is the Payment Card Industry (PCI) Data Security Standard

The Payment Card Industry (PCI) Data Security Standard is a new, single set of data security requirements, developed by Visa and MasterCard that will apply across the payment industry worldwide, and replaces the old AIS Standards and Best Practices, The AIS programme is based on the PCI Data Security Standard. The PCI Data Security Standard aligns Visa's original Account Information Security (AIS) and Cardholder Information Security (CISP) programmes with MasterCard's Site Data Protection (SDP) programme, resulting in a common set of industry tools and measurements that will ensure the safe handling of sensitive information and improve consumer confidence.

For more information on AIS and the Payment Card Industry (PCI) Data Security Standard go to www.visaeurope.com/acceptingvisa/ais or email: ais@visa.com.

Q3: Why is the new PCI standard necessary?

The PCI Data Security Standard provides a unified approach to safeguarding sensitive data across all card brands, and meets member, merchant and service provider business needs for a streamlined set of requirements across the payment industry. It also addresses merchants' and Acquirers' concerns about having to meet two sets of standards to accomplish a single goal.

Q4: What areas are covered by the PCI Data Security Standard?

The PCI Data Security Standard encompasses:
Technical Foundation: The Standard details technical requirements for the secure storage, processing and transmission of cardholder data.
Testing Methodologies: The Standard provides for common auditing procedures, scanning procedures and a common security Self-Assessment Questionnaire.
Vendor Certification: Vendor certification is cross-recognised; MasterCard has agreed to recognise Visa approved onsite security assessors, and Visa will recognise all MasterCard security scan vendors.

Q5: What are the compliance validation requirements for merchants?

The compliance validation requirements for all types of merchant are described in the table below.

Merchant Compliance Validation Requirements

Level	Selection Criteria	Validation Action	Validated By
1	Any merchant - regardless of acceptance channel - processing over 6,000,000 Visa transactions per year[1] Any merchant that has suffered a hack or an attack that resulted in a data compromise. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements in order to minimise risk to the Visa system Any merchant identified by another payment card brand as a Level 1.	■ **Annual Onsite Security Audit and** ■ **Quarterly Network Scan**	■ Independent Security Assessor or Internal Audit if signed by an officer of the company ■ Qualified Independent Scan Vendor[2] *Compliance validation is required no later than 30 June 2005*
2	Any e-commerce merchant processing 150,000 to 6,000,000 Visa transactions per year.	■ **Annual PCI Self-Assessment Questionnaire and** ■ **Quarterly Network Scan**	■ Merchant ■ Qualified Independent Scan Vendor *Compliance validation is required no later than 30 June 2005*
3	Any e-commerce merchant processing 20,000 to 150,000 Visa transactions per year.		

[1] The annual transaction volume for the previous 12 months from the date that the organisation started their AIS project or registered with a QSA.
[2] A Qualified Independent Scan vendor must be a MasterCard certified security vendor.

4	All other merchants, regardless of acceptance channel	■ **Recommended Annual PCI Self-Assessment Questionnaire and** ■ **Recommended Annual Network Scan**	■ Merchant ■ Qualified Independent Scan Vendor *Whilst compliance is mandatory for Level 4 merchants, compliance validation is not mandatory but strongly recommended.*[3]

[3] Acquirers are reminded that they are responsible for the compliance of their merchants and agents (*Visa International Operating Regulation*s section 2.2.E) and will be held liable for any financial losses resulting from a data compromise. Therefore it is strongly recommended that they require their level 4 merchants to carry out the recommended validation actions.

Q6: What are the compliance validation requirements for service providers?

The compliance validation requirements for all types of merchant are described in the table below.

Service Provider Levels and Compliance Validation Requirements

Level	Selection Criteria	Validation Action	Validated By
1	All VisaNet processors, payment gateways, and Internet Payment Service Providers regardless of transaction volumes	▪ **Annual Onsite Security Audit and** ▪ **Quarterly Network Scan**	▪ Qualified Independent Security Assessor ▪ Qualified Independent Scan Vendor *Compliance validation is required no later than 30 June 2005*
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually[4].	▪ **Annual Onsite Security Audit** ▪ **Quarterly Network Scan**	▪ Qualified Independent Security Assessor ▪ Qualified Independent Scan Vendor *Compliance validation is required no later than 30 June 2005*
3	Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 Visa accounts/transactions annually.	▪ **Annual PCI Self-Assessment Questionnaire** ▪ **Quarterly Network Scan**	▪ Service Provider ▪ Qualified Independent Scan Vendor *Compliance validation is required no later than 30 June 2005*

[4] The annual transaction volume for the previous 12 months from the date that the organisation started their AIS project or registered with a QSA

Q7: Aside from establishing a global set of security requirements, are there other specific benefits to the PCI Data Security Standard?

As part of Visa and MasterCard's alignment of security standards, merchants and service providers will be able to assess the status of their security by using a single validation process for all payment organisations. This will result in lower costs, reduced complexity and wider acceptance of standard security requirements for the industry. The alignment also allows merchants and service providers to select one vendor and implement a single process to comply with all payment card data security programmes.

Q8: When does the PCI Data Security Standard come into effect?

The new alignment of Visa and MasterCard's requirements, compliance criteria and validation processes will take effect immediately.

Q9: When must Merchants and Payment Service Providers begin using the new Payment Card Industry (PCI) Data Security Standard materials?

A: The Payment Card Industry Standards, Security Audit Procedures, Self Assessment Questionnaire and Security Scanning Requirements are effective immediately. However, for compliance validation assessments currently underway, the old AIS materials can be used.

Q10: When does the new validation requirement for annual service provider onsite audits become effective?

For service provider compliance validation annual renewals due before March 31st 2005, the old validation actions of a network security scan and Self-assessment questionnaire only can be used, as long as the service provider has not been identified as being of high risk due to a previous hack or compromise. The service provider must however use the new PCI Security Standard Security Scan procedures and Self-Assessment questionnaire.

For all annual service provider renewals due after 1 April 2005, and for all first time service provider assessments, an onsite audit is required.

Q11: What happens to Visa's Account Information Security (AIS) and MasterCard's Site Data Protection (SDP) programmes?

Visa's AIS and MasterCard's SDP programmes will continue to exist, but will adhere to the new PCI Data Security Standard.

Q12: If a Merchant or Service Provider has already been approved through the AIS programme, do they need to revalidate using the PCI Data Security Standard?

No, only at the time of their annual AIS compliance renewal. As AIS requires on going compliance validation, Members, merchants and service providers who have already been approved through the AIS programme, must consider

the new PCI Data Security Standard and the aligned compliance validation requirements as they prepare for their annual renewal.

Q13: How does Account Information Security affect merchants?

A: The Account Information Security (AIS) programme was developed to define protection requirements for the management of sensitive account and transaction Information in the Visa acceptance environment. The programme helps merchants protect their customers' information from hacking and fraud. Merchants ultimately benefit by lowering their liability, building a compelling reputation for transaction safety, and eliminating the possibility of damaging negative publicity due to compromise.

Q14: What risk is my business exposed to by not complying with the PCI Data Security Standard?

The PCI Data Security Standard is designed to assist organisations in protecting Visa account and transaction Information. Failure to protect account and transaction Information may result in financial loss due to fraud or a decrease in business caused by lower consumer confidence. Additionally, Acquirers may choose to penalise merchants, which, following a data compromise, are found to be non-compliant with the PCI Standard. Visa can enforce the PCI Standard using financial penalties and may require that specific actions be taken to protect account and transaction Information. In extreme circumstances, Visa may choose to revoke the acceptance privilege of a merchant or service provider that is found to have caused, through negligent behaviour, unnecessary hardship to the Visa system.

Q15: What should a merchant or service provider do if they suspect compromise?

Merchants and service providers fearing card and transaction details may have been compromised must:

- Act immediately to contain and limit the exposure, to prevent the further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation, whenever possible, Merchants should not access or alter compromised systems, but rather isolate compromised systems from the network. They should preserve all logs and electronic evidence of the compromise, and log all actions taken.
- Contact their Acquiring bank immediately, providing all necessary information, including all account numbers feared compromised, the time window of the possible compromise.
- Contact the local police/security agency if the compromise is believed to be of criminal nature
- Follow further instructions from the Acquiring bank

Q16: Is there a deadline for certification with AIS?

The new compliance validation requirements for AIS require that merchants and service providers validate their compliance with the PCI Data Security Standard by 30 June 2005.

Q17: In what way am I responsible as an Acquirer?

It is the Acquirer's duty as a Member of Visa to ensure that all their Merchants and agents are compliant. If a Merchant/agent is victim of a compromise, and it is confirmed that the compromise is due to non-implementation or partial implementation of the AIS Programme, the Acquirer will be deemed responsible by the Visa membership, and Visa EU may fine the Acquirer for AIS non-compliance, at a rate of 5 euros per compromised account (VISA EU Operating Regulations 2.5).

Q18: Is AIS only for e-commerce merchants?

No. AIS is for all Merchants. Under the AIS Programme, Acquirers are liable for compromise taking place at any of their Merchants and agents (VIOR 2.2.E.1).

Q19: How do I as an Acquirer self-certify my compliance status?

Acquirers and Processors can self-certify their compliance status annually by completing the 'AIS Self-Certification' form and confirming whether they are compliant, partially compliant, or non-compliant. A compliant Acquirer is one that has validated that their merchants and agents are compliant in accordance with the AIS Compliance Validation Requirements for Merchants and Service Providers. All non-compliant and partially compliant Acquirers have to submit an action plan to Visa EU, which will review it for appropriateness and effectiveness and confirm acceptance.

Q20: How do I as a service provider become certified with the AIS programme requirements?

A service provider needs to contract with an independent vendor or QSA to perform their assessment. The results of service providers' assessments will need to be sent to Visa, and to the Acquirer if they require it. If there are no non-compliances found, Visa will approve the service provider's scan, audit or Self-assessment questionnaire report and list the service provider as 'Certified' on the Visa website. If some non-compliances are found, Visa will request that service provider addresses the non-compliances in an action plan that will be monitored until completion.

Q21: How do I as a merchant become certified with the AIS programme requirements?

Merchants must contact their Acquirer to determine the method and approach by which they will become certified. The Acquirer may suggest a vendor for

the merchant to contract with to provide AIS validation services. Acquirers will inform Visa of their merchants' compliance status on the annual self-certification statement.

Q22: How long will the certification process take?

This depends on whether a merchant or service provider requires an audit, or a questionnaire. It is recommended that the whole process takes no longer than 60 days from start to finish. If an organisation takes longer than 60 days to complete their assessment, it is possible that their current assessment will be cancelled and they may need to start again.

Q23: Where can I find more information on Visa Europe's AIS programme?

For more information on Visa Europe's AIS programme, go to www.visaeurope.com/acceptingvisa/ais or email: ais@visa.com.