



Account Information Security

When customers offer their payment card at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. This is the reason why Visa CEMEA has implemented the Account Information Security programme (AIS).

It is a globally mandated programme that is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, payment processors and service providers maintain the highest information security standard.

Using the Payment Card Industry (PCI) Data Security Standard as its framework, the AIS programme provides the tools and measurements needed to enable members, merchants, payment processors and service providers to achieve compliance.

If you are an entity based outside Visa CEMEA region, please visit [Visa International Account Information Security \(AIS\)](#)

1. **AIS Programme overview** – An overview of Visa CEMEA AIS programme, and entities it applies to
2. **The PCI Data Security Standard** – The requirements of the Payment Card Industry Data Security Standards.
3. **Benefits of the AIS programme** - How the programme benefits your organisation and adds value to your business
4. **AIS compliance validation tools** – Outlines the tools used to measure compliance and who can validate compliance
5. **AIS compliance validation threshold** - An explanation on how your organisation can achieve the AIS programme compliance
6. **In case of a compromise** – What to do in case of a security incident
7. **Downloads and resources** – Useful AIS documents.
8. **Qualified Security Assessors**
9. **Programme registration**

1. AIS Programme Overview

Visa International introduced the Account Information Security (AIS) programme in September 2000. The AIS programme was globally mandated in 2001. Visa was the first payment scheme to define a set of security standards and best practices designed to protect the confidentiality, availability and integrity of stored customer account and transaction data. Compliance with the AIS programme provides members across the globe with the confidence that acquirers, their merchants and service providers are safely storing account and transaction data.

Alignment of standards

In response to requests from members, merchants, and service providers for stronger information security standards and a single approach to safeguarding sensitive data for all card brands, Visa and MasterCard have collaborated in creating common industry security requirements. The alignment of Visa's Account Information Security programme (AIS) and MasterCard's Site Data Protection (SDP) programme has led to the formation of a worldwide standard for consumer data protection across the payment industry that is known as the Payment Card Industry (PCI) Data Security Standard.



The new PCI Data Security Standard v1.1 has been released and is now available. With effect from 7 September 2006, the PCI Security Standards Council ("PCI SSC") owns, develops, maintains and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Visa CEMEA however, will continue to manage all compliance enforcement and validation initiatives for the regional AIS Programme.

Visa CEMEA's QSA Programme has also been transferred to the PCI SSC. Please refer to the Qualified Security Assessor page for more information.

Entities the PCI Data Security Standards applies to

Compliance to the AIS Programme is required of all entities that store, process, or transmit Visa cardholder data. The programme applies to all payment channels, including retail (bricks-and-mortar), mail/telephone order, and e-commerce. This includes Visa Members, merchants, third party processors, gateways and Internet payment service providers, and other third party service providers such as network providers, data consolidators, media back-up companies, and web hosting companies.

It is the responsibility of Visa Members to ensure the compliance of their merchants, service providers, and any other agents utilised for payment processing.

2. The Payment Card Industry Data Security Standards

The PCI Data Security Standards consists of twelve basic requirements supported by more detailed sub-requirements:

PCI Data Security Standards

Build and maintain a secure network	Requirement 1. Install and maintain a firewall configuration to protect data
	Requirement 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	Requirement 3. Protect stored data
	Requirement 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a vulnerability management program	Requirement 5. Use and regularly update anti-virus software
	Requirement 6. Develop and maintain secure systems and applications
Implement strong access control measures	Requirement 7. Restrict access to data by business need-to-know
	Requirement 8. Assign a unique ID to each person with computer access
	Requirement 9. Restrict physical access to cardholder data
Regularly monitor and test networks	Requirement 10. Track and monitor all access to network resources and cardholder data



	Requirement 11. Regularly test security systems and processes
Maintain an information security policy	Requirement 12. Maintain a policy that addresses information security

3. Benefits of the AIS Programme

By implementing and adhering to the AIS requirements, Visa Members, merchants, and service providers not only meet their obligations to the Visa payment system, but also build a culture of security that benefits everyone.

Benefits of the AIS programme include:

- It limits risk associated with data compromise and fraud
- It improves confidence in the payment industry
- It protects reputation
- It promotes brand integrity
- It boosts consumer confidence
- It provides competitive edge
- It increases revenue and improves bottom line

4. AIS Compliance Validation Tools

The AIS programme uses a set of tools and measurements that are common to the payment industry. Members, merchants, and service providers can assess the status of their security by using a single validation process for all card companies. The alignment also allows members, merchants and service providers to select one vendor and implement a single process to comply with all payment card data security programmes. This will result in wider acceptance of standard security requirements for the industry, reduced complexity, and lower costs.

Please refer to the section on AIS Compliance Validation Threshold to identify the compliance validation tool and validation cycle applicable to your organisation.

Please visit the Download and Resources Section to download the validation tools.

Validation tools

1. Payment Card Industry Self Assessment Questionnaire

The Self-Assessment Questionnaire is a free, confidential tool that can be used to gauge your compliance with the PCI Data Security Standards. The Self-Assessment Questionnaire is divided into six sections, each focusing on a specific area of security, based on the requirements included in the PCI Data Security Standards. Members, merchants and service providers are required to fill in a rating box upon completing each section to determine compliance.

2. Payment Card Industry Security Scanning Procedures



The Payment Card Industry Security Scanning Procedures provide guidelines for conducting network security scanning in compliance with the PCI Data Security Standards.

The document is intended for entities that are required to scan their infrastructure to demonstrate compliance.

To support the efforts of entities validating compliance Visa Cemea has contracted One-Sec Limited to provide a free on-line self-assessment and vulnerability scan for qualifying entities. Please log on to the website below to register and use this free service.

<http://visacemea.one-sec.com>

3. Payment Card Industry Security Audit Procedures

The Payment Card Industry Security Audit Procedures document is used to validate compliance of entities that are required to undergo an on-site audit. Where applicable, such entities are required to use the document to perform an on-site audit of all system components where cardholder data is processed, stored, or transmitted.

Who can validate compliance?

Self-assessment

Self-assessment can be performed by any entity that is interested in establishing its compliance to the PCI Data Security Standards.

Scanning and on-site audit

It is a requirement of the AIS programme that network infrastructure scanning, and on-site audit is performed by Qualified Security Assessors. Please refer to the section on [Qualified Security Assessors](#) for further information.

5. AIS compliance validation threshold

Visa CEMEA has prioritised and defined thresholds of AIS compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the Visa system by members, merchants and service providers. The compliance validation tool and validation cycle is defined within each threshold.

The number of validation tasks that should be completed depends on the number of Visa accounts stored, processed or transmitted on a yearly basis. Those entities that process or store large volumes of cardholder account and transaction information provide a greater exposure to all parties (should a compromise occur), and thus need to perform a more in-depth compliance validation. The table below shows which validation tasks need to be completed, based on your annual Visa transaction volume.

Service provider levels defined

Service providers are organisations that process, store, or transmit Visa cardholder data on behalf of Visa members, merchants, or other service providers. Service provider levels are defined as:

Service provider level	Description	Validation Required	Deadline !
------------------------	-------------	---------------------	------------



1	All VisaNet processors (member and Nonmember) [†] and all payment gateways*	(1) Annual on-site audit (2) Quarterly network scan	31 st Dec 2006
2	Any service provider that is not a Level 1 and stores, processes or transmits more than 1,000,000 Visa Account/transactions annually	(1) Annual on-site audit (2) Quarterly network scan	31 st Dec 2006
3	Any service provider that is not a Level 1 and stores, processes or transmits fewer than 1,00,000 Visa Account/transactions annually	(1) Annual Self assessment Questionnaire (2) Quarterly network scan	31 st Dec 2006

+ Visanet processors are a non-member or member owned entities which have direct connection into VisaNet.

- Payment gateways are a category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction. Specifically, they enable payment transactions (e.g., authorization or settlement) between merchants and processors (VisaNet endpoints). Merchants may send their payment transactions directly to an endpoint, or indirectly to a payment gateway.
- ! Deadlines are set by Visa based on annual validation cycle. Please refer to member letter Cemea 33/06 for 2007 deadline.

Merchant levels defined

These levels only apply to merchants who have the capability to store, transmit or process cardholder data electronically.

Merchant Level	Description	Validation Required	Deadline
1	Any Merchant who stores, processes or transmits more than 6 Million Account/transactions annually	(1) Annual on-site audit (2) Quarterly network scan	31 st Dec 2006
2	Any Merchant who is not a Level 1 and stores, processes or transmits up to 6,000,000 Visa Account/transactions annually	(1) Annual Self assessment Questionnaire (2) Quarterly network scan	31 st Dec 2006

*The PCI DSS requires that all merchants perform external network scanning to achieve compliance. Acquirers may require submission of scan reports and/or questionnaires by Level 2 merchants.

- ! Deadlines are set by Visa based on annual validation cycle. Please refer to member letter Cemea 33/06 for 2007 deadline.

6. In case of a compromise

A Member or the Member's service provider, or a merchant or the merchant's service provider must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

If a Member knows or suspects a security breach at a merchant or service provider, the Member must take immediate action to investigate the incident and limit the exposure of cardholder data.

The Member responsible for the organisation that has suffered the compromise must provide Visa with all the information on the compromise including the range of account information that has or may have been stolen, details of the organisation where account data was stolen, and Member's actions taken to investigate and address the issues that caused the compromise. Visa may request that the Member employ an independent security company to perform a forensic investigation at the Member's expense.



Useful tips

If you experience a suspected or confirmed security breach, you should:

1. Immediately 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:

- Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT)
- Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable)
- Preserve logs and electronic evidence
- a backup should also be performed on the system to maintain the current state of the system to facilitate the post-mortem and forensic investigation later
- Log all actions taken
- If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised)
- Be on HIGH alert and monitor all Visa systems.

2. Contact the Visa Cemea AIS Management Team at:

Tel: + 44 (0) 20 7225 8724

Fax: + 44 (0) 20 7225 8513

Email: CemeaAIS@visa.com

7. Downloads and resources

The following documents provide useful information on Visa CEMEA's AIS programme and the PCI Data Security Standard. The standard and all related documents listed below can be downloaded from the Payment Card Industry Security Standard Council's website.

<https://www.pcisecuritystandards.org>.

[Payment Card Industry \(PCI\) Data Security Standards](#)

[Payment Card Industry Self-Assessment Questionnaire](#)

[Payment Card Industry Security Scanning Procedures](#)

[Qualified Security Assessors](#)

8. Qualified Security Assessors



The ownership and management of Visa CEMEA's QSA Programme has also been transferred to the PCI Security Standards Council ("PCI SSC") with effect from 7 September 2006.

All potential assessors wishing to perform PCI Data Security Assessments for merchants and service providers must be approved by the PCI SSC as a Qualified Security Assessor

("QSA"). Please visit the [PCI Security Standards Council](#) for details on the QSA Programme, requirements, updated training schedules and related information.

PCI validation assessments performed by qualified security assessors, have become increasingly critical in today's environment. The proficiency with which a QSA conducts an assessment can have a tremendous impact on the consistent and proper application of measures and controls compliant with the PCI Data Security Standard. Assessors performing PCI Data Security Assessments for merchants and service providers must be approved as a Qualified Security Assessor.

Visa CEMEA QSAs are listed at: <https://www.pcisecuritystandards.org>

The cost of compliance validation varies, based on the vendor of choice, and the number and size of merchants and service providers. Visa is not involved in the pricing of security assessments. For more information, contact the Qualified Security Assessor of your choice.

9. Programme registration

If your organisation operates within Visa CEMEA region or provide services to a Visa member bank located within Visa CEMEA region, and are required to undertake compliance validation for the AIS Programme, please complete a copy of the AIS Contact Form and return it to the Visa Cemea AIS Management Team at the email address above.