



Account Information Security (AIS) Vulnerability Scan Service Users' Guide

September 2005

VISA PAYMENT SECURITY SERVICES
ASIA PACIFIC



About Visa Asia Pacific's AIS Scanning **VISA** Service

As part of Visa Asia Pacific's Account Information Security Program (AIS), which helps protect sensitive cardholder account and transaction information, Visa Asia Pacific is offering a **FREE** security assessment service for all parties that handle Visa cardholder data, such as service providers, Internet Payment Service Providers (IPSPs) and merchants.

The service includes self-assessment and vulnerability scanning of your network.

ScanAlert, one of the world's largest website security certification companies will provide the free security assessment and validation service. ScanAlert will also provide Visa's member financial institutions in the Asia Pacific with a comprehensive reporting system to track the AIS validation status of their merchants and service providers.





Getting Started



Logging onto AIS Scan Portal



ScanAlert™

.. CUSTOMER LOGIN .. English

Making the web HACKER SAFE®

We make websites safe from hackers and certify it to their customers

FIND HACKER SAFE SITES

WARNER BROS. STUDIOS

SHOPPERS

MERCHANTS

GOVERNMENTS & NON-PROFITS

PROFESSIONAL SERVICES

PARTNERS

TECHNOLOGY

COMPANY

Over 65,000 Web sites use HACKER SAFE® certification to help protect you from identity theft and credit card fraud.

Wouldn't you rather shop at a HACKER SAFE site?

View demo to learn more . . .

ScanAlert™ HACKER SAFE TESTED 16-AUG

PCI COMPLIANCE CISP / AIS / SDP

VISA Visa Asia Pacific AIS validation service

[Click here to sign-up for PCI certification service](#)

- Open your web browser and enter: www.scanalert.com
- Click on the link:

Visa Asia Pacific AIS Validation Service



At the Welcome Page



Welcome to the Visa Asia Pacific Account Information Security Portal

If you have already enrolled [click here to Login](#)

Visa Asia Pacific has partnered with ScanAlert, the world's leading web site security certification company, to sponsor **FREE Visa AIS validation services** for all Asia Pacific region Internet Payment Service Providers (IPSP) and merchants.

Visa's Account Information Security Program (AIS) is a Risk Management program sponsored by Visa and run by Visa's members. The AIS program is a requirement for all entities, such as merchants and service providers, that process, store or transmit Visa cardholder account and/or transaction information.

To check whether your organization meets the required AIS standards, you need to complete the following validation tasks (depending on the average monthly Visa volume you process):

- Self-Assessment Questionnaire (<10k transactions)
- Quarterly Vulnerability Scan (between 10k and 50k transactions)
- Onsite Review (>50k transactions)

Through Visa's sponsorship, Asia Pacific region IPSPs and merchants can access ScanAlert's AIS validation service at no cost. ScanAlert's easy-to-use self-assessment questionnaire "Wizard" and safe, non-invasive security scanning enables many participants to successfully validate within a few hours of enrollment.

The program provides all of the services you need:

- Online assistance completing your self-assessment questionnaire
- Safe vulnerability scans of all Internet servers and network connection points
- Assistance preparing your AIS compliant security policy
- Telephone technical support (for vulnerability scanning only)
- Preparation of your "AIS Valiation Report" upon completion
- Service available in English and Mandarin Chinese

Only Asia Pacific region IPSPs and merchants are eligible for the FREE Visa AIS Validation Service. Please click "Continue" to sign up now.

Enrollment Code (Optional)

If you have an enrollment code please enter it here and click "Validate."

Visa Asia Pacific AIS Validation - 100% Off

Sign Up Now

Your Visa AIS Validation account includes scanning of up to six devices. You may add more devices to scan after you enroll. Click "Continue" to sign up now.

Scanning	Included	Additional
Device - Quarterly	6	<input type="text" value="0"/>

- You will be brought to a Welcome Page – read this first then:
- **Click Continue**

Enrollment



Thank you for choosing Visa Asia Pacific's AIS Validation Service.

After completing the form below you will receive an email containing login instructions. Once logged into our AIS Portal you will find easy-to-follow instructions for completing the Self-Assessment Questionnaire, adding devices for security scans, and completing all other steps necessary to obtain a Validation Report.



Company Information

Company Name	<input type="text" value="AIS Service Test"/>
Phone	<input type="text" value="+61 2-5555-1111"/>
Address	<input type="text" value="2 Main. St.,"/> <input type="text"/> <input type="text"/>
City	<input type="text" value="Sydney"/>
Country	<input type="text" value="Australia"/>

Login

First Name	<input type="text" value="Nigel"/>
Last Name	<input type="text" value="Ravenhill"/>
Email	<input type="text" value="raventhewriter@yahoo.com"/>
Phone	<input type="text" value="+61 2-5555-1111"/>

PCI Audit Terms

Terms and Conditions for provision of Payment Card Industry Data Security Standard (PCI) compliance audit to be provided by ScanAlert, Inc., a PCI compliant network security scanning vendor.

1. Acknowledgement

1.1 By using the web site on which this document is found ("the Site"), you acknowledge

- The enrollment page appears
- Enter your company information
- Upon completion of the fields, read the PCI Audit Terms. You are legally bound by these terms, which describe your responsibilities and how you may use the system.
- Then click **Complete**

ScanAlert AIS Portal



- You would receive a welcome email with the Subject header: **“ScanAlert – FREE Asia Pacific AIS Validation”** upon enrollment
- Click on the link in the email
- Use the temporary password provided in the email to login to the ScanAlert’s AIS Portal
- Additional links such as **FAQ** and **Best Practices** are located on the toolbar on the left-hand side of the page.



Self-Assessment Questionnaire (SAQ)



Completing the Self-Assessment Questionnaire



ScanAlert Security Management Console

Security Account Tools PCI Logout

Validation
Get Started
How We Scan

Information
FAQ
Best Practices

1 Self-Assessment 2 Security Scanning 3 AIS Validation Report

Welcome to the PCI Self-Assessment Questionnaire (SAQ) Wizard

When completing the PCI Self-Assessment Questionnaire (SAQ) please keep in mind that it specifically addresses your business practices, computer systems and Web site(s) that are directly involved in processing, storing, or transmitting payment card data.

The Wizard will assist you in completing the questionnaire by filling in sections of the questionnaire for you, based on your answers to a few simple preliminary questions.

After completing the 7 Wizard sections below you simply indicate YES, NO or N/A answers to any self-assessment questions not already answered YES by the Wizard.

*Click the "Save Changes" button at the bottom of this page at any time to save your work for completion later. If your session times-out while working on the form, please log back in at the login prompt to resume.

1. Organization Information

This is your company or organization's merchant banking contact information.

Corporate Name	AIS Service Test
DBA	N/A
Contact Name	Nigel Ravenhill
Contact Title	Unknown
Contact Phone	+61 2-5555-1111
Contact Email	raventhewriter@yahoo.com

- To commence the Self-Assessment Questionnaire (SAQ), click on the **Self-Assessment** button
- An SAQ wizard will be launched

SAQ Wizard



7. Preliminary Questions

Answering these questions will determine which sections of the questionnaire the Wizard can complete for you. If you can accurately answer "No" to any of questions 1, 2, 3, 4, or 6 your compliance requirements will be greatly reduced. Answering "Yes" to question 5 about daily scans meets the requirements for an Intrusion Detection/Prevention system. Please be sure you answer these questions accurately.

NOTE: If you answer "Yes" to questions 1 or 2 you will need to change your business practices in order to meet the PCI security standard requirements. PCI standards require that you do not store un-encrypted card data in your place of business or on your web site, or allow access to full numbers that are stored.

*You must click the "Grade" button at the bottom of this page each time you make changes to your Wizard answers.

Question	Yes	No	N/A
1. Do you store un-encrypted (in clear text) payment card information <u>anywhere</u> in your business operations, either in writing, on computers, or on your web site? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. Are stored payment card numbers (full 16 digits) accessible by any personnel? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Do you have an in-house software development team that produces your transaction software? (most small businesses do not do this) Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Are there any POS devices (other than your website) that are connected to a computer network within your business? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. Is your website scanned daily through the HACKER SAFE certification program? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. Do you have a wireless network or wireless access points directly connected (not through the Internet) to a local network containing any POS devices, payment processing terminals, or payment card data storage systems? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

- Based on your answers to a few simple preliminary questions, the SAQ wizard will automatically pre-complete certain sections of the questionnaire for you.
- The wizard will also provide a sample Payment Card Industry (PCI) compliant Information Security Policy

Online Help



Requirement 1 Of 12:			
Install and maintain a firewall configuration to protect data	Yes	No	N/A
Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards? ▶ Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
If wireless technology is used, is the access to the network limited to authorized devices? ▶ Explanation	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Do changes to the firewall need authorization and are the changes logged? ▶ Explanation	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Is a firewall used to protect the network and limit traffic to that which is required to conduct business? ▶ Explanation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Are egress and ingress traffic inspected for impersonation with spoofed IP addresses?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Is payment card account information protected on the network (not the DMZ)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
If wireless technology is used, are wireless networks and the payment card account information protected?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Does each mobile computing device have a firewall and anti-virus software installed and updated?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

ScanAlert - Microsoft Internet Explorer

Enable encryption and MAC filtering on your wireless network to prevent unauthorized devices from accessing it.

How to meet this requirement: If you have a wireless network, enable encryption and MAC filtering. Your Configuration Policy should state that these security features are required.

[▶ Close Window](#)

- Click **Explanation** if you need more information on the question

12.5 Is there an up-to-date information security awareness and training program in place for all system users? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.6 Are employees required to sign an agreement verifying they have read and understood the security policies and procedures? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.7 Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.8 Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.9 Is a security incident response plan formally documented and disseminated to the appropriate responsible parties? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.10 Are security incidents reported to the person responsible for security investigation? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
12.11 Is there an incident response team ready to be deployed in case of a cardholder data compromise? Explanation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

After completing the 12 sections above save and download your completed questionnaire. Certain answers to questions in this questionnaire have been pre-populated based on information you have supplied to ScanAlert. You must review each question in this document for accuracy before submitting the results to your bank or Visa. ScanAlert accepts no responsibility for the accuracy of these pre-populated answers.

Your Results

You must complete 100% and pass 100% to be compliant with the PCI requirements

Completed 100%

Passed 100%

Grade

>> Save Changes <<

>> Download SAQ Form <<

- There are 12 sections in the SAQ. (Note: All questions must be answered in order to receive an AIS Validation Report)
- Click **Grade** at any time to see how close you are to finishing the SAQ.
- Once you have completed all questions and receive a 100% compliant grade, click **Save Changes**. (You may also save changes at any time to save your work for completion later)
- Click **Download SAQ Form** to download your SAQ for future reference.

NOTE: To be compliant with the PCI standards, obtain a 100% pass grade.

Vulnerability Scanning



Getting a Security Scan



ScanAlert Security Management Console

VISA

Security Account Tools PCI Logou

Validation
Get Started
How We Scan

Information
FAQ
Best Practices

1 Self-Assessment 2 Security Scanning 3 AIS Validation Report

Security scanning is required for all Internet servers and network connection points involved in collecting, processing, transmitting or storing cardholder data. This includes office connections (dial-up modem, DSL, cable or wireless), store locations and Internet servers such as website(s), email, FTP, etc.

Click "Add Device" to enroll the domain names or IP addresses to be scanned.

To scan Dynamic IP Addresses, such as dial-up modem, DSL or cable Internet office/store connections click on the "Security" tab at the top of this page, then click on "Dynamic IP" under the "Vulnerability" menu item.

Note: After adding devices you must contact your regional ScanAlert representative to "Activate" scanning. Users in Taiwan or Hong Kong please call +886-2-2700-2207. Users in Australia, New Zealand or other Asia Pacific countries please call +61 2 9922 6988 or +61 2 9929 0188.

Add Device

- Click on the **Security Scanning** button
- For more information on ScanAlert's scanning technology, click **How We Scan**
- Click **Add Device** to add devices to be scanned.

Adding a Device



ScanAlert Security Management Console

VISA

Security Account Tools PCI Logout

Add Device

To add a device to be scanned enter its domain name or IP address below.

Domain names that resolve to multiple IP addresses will automatically receive a separate device entry for each IP address.

Scan Schedule

Quarterly Scanning - Using 0 Of 6

Domain or IP Address

www.sydneypay.com

I agree to ScanAlert's [Terms of Service](#)

I understand that improper use could damage and/or cause interruptions of service to this device

Add Device

- Enter each domain or IP address that requires scanning. (You must accept ScanAlert's Terms of Service prior to the scan)
- Click **Add Device** to add a device to be scanned. Prior to adding a device, you must call a ScanAlert representative to activate scanning

For Taiwan or Hong Kong, please call +886-2- 88726875 or email aistaiwan@scanalert.com

For all other Asia Pacific countries, please call +61-2-94202070 or email ais_au@scanalert.com.



AIS Compliance Report



Obtaining an AIS Compliance Report



- To obtain a AIS Validation Report, you must:
 - Answer all questions
 - No Level 3,4,5 vulnerabilities identified from scan

- Validation Reports are available in a HTML or PDF format.



For any inquiries with regards
to AIS scan, please contact

Visa Payment Security
Services
Asia Pacific

APrisk@visa.com

www.visa-asia.com/secured