



**Visa Asia-Pacific**  
**Additional Information Requirements for Security Reviews**  
**by non Visa QSA's**

---

Agents that have AIS or other information security assessments performed on their Visa processing environments by other than a Visa QSA (Qualified Security Assessor) must prepare a report containing the following topics and information.

Visa will determine from this report if the requirements of AIS Certification have satisfactorily been met. Visa's decision is final.

**1. Executive Summary**

Include the following:

- Business description
- Environment in which the assessment was focused (i.e., client's Internet access points, internal corporate network). *Visa Asia-Pacific requires an assessment to be performed on systems that handle and/or store cardholder information.*
- Any service provider relationships or entities with whom the company shares cardholder data and their AIS compliance
- Any wireless LANs connected to the cardholder information processing environment
- Any wireless POS terminals and internet connected POS terminals connected to the cardholder information processing environment

**2. Description of Scope of Work and Approach Taken**

- The depth to which assessment was performed and a high-level overview of the methodology. Include here which standard/s the entity was audited against.
- Timeframe of assessment
- List of those interviewed e.g. Head of HR, Head Information Security Office, firewall administrator etc.
- List of documentation reviewed

**3. Findings and Observations**

- Describe tests performed other than Visa Security Audit Procedures (SAP) for the requirements.
- Summary of findings (in table format, see overleaf)

**4. Contact Information and Report Date**

- Include select merchant or service provider and security firm contact details.
- Date of report



**Example of summary of compliance for: ACME Processing Inc.**

<b>Requirement</b>	<b>In place</b>	<b>Not in place</b>	<b>Comments</b>
1. Establish a hiring policy for staff and contractors	✓		
2. Restrict access to data on a "need to know" basis	✓		
3. Assign each person a unique ID to be validated when accessing data	✓		
4. Track access to data, including read access, by each person	✓		
5. Install and maintain a network firewall, if data can be accessed via the Internet	✓		
6. Encrypt data maintained on databases or files accessible from Internet	✓		
7. Encrypt data sent across networks		✓	All employees to have secure email capability within 30 days
8. Protect systems and data from viruses	✓		
9. Keep security patches for software up-to-date	✓		
10. Don't use vendor-supplied defaults for system passwords and other security parameters	✓		
11. Don't leave papers/diskettes/computers with data unsecured	✓		
12. Securely destroy data when it's no longer needed for business reasons		✓	Secure document destruction bins to be supplied for each business unit in 30 days
13. Regularly test security systems and procedures	✓		
14. Immediately investigate and report to Visa any suspected loss of Account or Transaction information		✓	Visa "Incidence Response Guidelines" to be employed within 30 days
15. Use only service providers that meet these security standards	✓		