



NetAUDIT™ PCI On-site Security Assessment

Payment Card Industry Data Security Standard
and VisaUSA CISP compliance services

Companies may be shielded from possible fines if found compliant at time of breach

The Payment Card Industry (PCI) has approved Data Security Standards for all Merchants and Payment Service Providers who store, process or transmit cardholder data.

The standards are designed to protect the overall payment system, infrastructure, and cardholder data against the threat of compromise. It does this by requiring regular inspection of internal security controls to validate compliance with VisaUSA Cardholder Information Security Program (CISP) requirements.

PCI CISP security standards have been accepted by most major credit card companies, who, in turn, require businesses that accept, store, process, and/or transmit credit card data to meet respective on-site security assessment requirements.

Merchants averaging 20K to 6M transactions annually and Payment Service Providers with less than 1M annually must perform a self assessment or use a third party. Those with more transactions are required to use a QDSC and Merchants may optionally perform an internal assessment signed by an officer of the company.

Companies that are found to be in compliance with PCI CISP requirements at the time of a breach may avoid:

- Fines
- Public scrutiny
- Reputation damage
- Possible removal from card acceptance programs

Spohn is a QDSC for CISP Assessment

Spohn Consulting, Inc. is one of a limited number of Qualified Data Security Companies (QDSC) authorized to perform PCI on-site security assessments in accordance with the VisaUSA Cardholder Information Security Program. We strive to partner with our clients as well as be a resource to:

- Validate PCI CISP compliance
- Minimize an intruder's incentive by identifying and limiting the enticements that lead to probing of systems
- Maintain a system of security controls by identifying and improving weaknesses so that it is less susceptible to actual intrusion and better prepared to recover from an attack
- Provide check-and-balance to prevent costly mistakes

NetAUDIT assessment identifies security vulnerabilities and validates compliance

Even though mandatory compliance dates have passed, many companies have not met PCI annual assessment requirements because they don't have the guidance, resources, time or funding to effectively prepare for or perform an assessment. Engaging external assistance and outsourcing this function to a qualified assessor is a feasible and beneficial alternative.

NetAUDIT PCI On-site Security Assessment services provide the guidance, engineers, tools, processes, analysis, and recommendations for improving security controls and validating compliance.

Benefits

- **Protect customer information**
- **Avoid fines and other losses resulting from a security breach**
- **Remain in compliance with PCI Data Security Standard for network assessment**
- **Pre-flight your Validation and prevent the submissions of a Fail result to Visa**
- **Improve maintenance of security operations through remediation assistance**
- **Maximize security investments by leveraging certified security knowledge and expertise**

NetAUDIT Self Assessment Assistance

Merchants and Service Providers that are required or recommended to perform a self assessment using VisaUSA's Self Assessment Questionnaire may need additional help to ensure that they properly assess their organization. NetAUDIT will help you to:

- Complete the Self Assessment Questionnaire
- Identify vulnerabilities in your security controls
- Remedy identified problems
- Better plan and manage your security investments

NetAUDIT Pre-Validation Assessment

Many merchants and service providers are unsure of their system's level of compliance and may not be ready for Validation and Visa notification of Pass/Fail status.

Pre-Validation Assessment can determine your gap in PCI compliance and provide the data and recommendations to bring controls in line with requirements prior to Validation. Pre-validation Assessment provides the following key services:

- Inspection of security controls against Visa CISP requirements
- Gap Analysis of non-compliant areas
- Identification of vulnerabilities
- Remedy recommendations and guidance on compensating controls
- Remediation Database for in-house analysis and remediation planning
- Consultation and guidance in preparation for Validation

The scope of the pre-validation assessment for merchants includes:

- All external connections into the merchant network

- All connections to and from the authorization and settlement environment
- Any data repository outside the authorization and settlement where more than 5,000 account numbers are stored
- IP-based POS environment with external access via Internet, VPN, dial-up, broadband or publicly accessible machines to the merchant location

The scope of pre-validation assessment for service providers is:

- Any system(s) or system component(s) involved in storing, processing, or transmitting Visa cardholder data.

Findings are kept confidential and are not reported to VisaUSA.

NetAUDIT PCI Compliance Validation

Compliance Validation service inspects security controls per CISP requirements and a pass/fail report is provided to Visa.

Although VisaUSA offers a list of companies to provide this service, NetAUDIT includes the following additional benefits:

- A central point of contact to manage Validation efforts throughout your organization and with VisaUSA
- Status reports during the Validation process
- Consultation and guidance on PCI CISP Validation requirements and process
- Post-Validation remedy recommendations for gaps found

Tailor your assessment to meet other goals

NetAUDIT may be tailored to help you meet any number of requirements within a single on-site assessment. Contact us to design a custom NetAUDIT service.

Features

- Quick turnaround for global pass/fail results
- Single point of contact to Visa for your validation
- Prioritized report of vulnerabilities with detail of problems and solutions
- System misconfigurations are identified
- Industry strength scanning tools for deep inspection of external facing devices
- Assessment of current threats and probabilities
- Documentation review with staff for explanation of findings and recommendations
- Documentation provided in print and on CD-ROM

Spohn's NetAUDIT PCI Network Security Assessment is a member of a suite of security products designed to assist companies in protecting their data and meeting regulatory compliance.

For further information please contact our corporate office at 512.685.1000

Visa USA CISP Validation Actions

Group	Level	Annual Transactions	On-site Security Audit	Self Assessment Questionnaire
Merchant	1	> 6M	Required Annually	
	2 & 3	20K - 6M		Required Annually
	4	< 20K		Recommended Annually
Service Provider	1	VisaNet processors and payment gateways	Required Annually	
	2	> 1M	Required Annually	
	3	< 1M		Required Annually