



## The Payment Card Industry Data Security Standard (PCI DSS) Frequently Asked Questions

### Q: What is the PCI DSS?

A: The PCI DSS outlines the requirements set forth by the PCI Council, an open global forum for the enhancement of payment account data security, for safeguarding credit card data wherever it is stored, processed or transmitted. As such, the new standard contains IT security requirements and guidelines for **all major credit card issuers**, including Visa, MasterCard, American Express, Diners Club and Discover.

**The PCI DSS consolidates and supersedes the requirements of the previously developed MasterCard Site Data Protection (SDP) Program and the Visa Cardholder Information Security Program (CISP).**

### Q: When did the standard go into effect?

A: Dec. 14, 2004.

### Q: Who is required to demonstrate compliance with the PCI DSS?

A: All merchants and service providers who store, process, or transmit cardholder data. There are specific requirements set out by the level assigned to merchants and service providers which is dependant on the quantity of credit cards received/processed annually. Please see page two for details on each level.

### Q: How do I determine what level I am?

A: As noted above, the level is dependant on the quantity of credit card transactions your organization receives or processes annually, and this quantity is comprised from a total across all the major credit card brands. If you need direction in defining your level, please contact your acquiring bank as they will be able to inform you of your PCI DSS requirements.

### Q: When must merchants demonstrate compliance with the standard?

A: Most merchants and service providers were required to comply with this standard by **June 30, 2005** or face penalties, including fines and loss of the ability to accept credit cards. New requirements are being added; e.g. PCI DSS 6.6 is effective June 2008.

## ACCELERATE AND SIMPLIFY PCI COMPLIANCE

### Q: What are the requirements of the PCI Data Security Standard?

A: Requirements of the PCI standard involve two key steps in the compliance process:

1. Pass **quarterly vulnerability scans** on all systems that comprise the credit card data infrastructure. External, Internet-facing system components **must** be assessed by an Authorized Scanning Vendor (ASV) such as Solutionary,


**Solutionary, Inc.** 9420 Underwood Avenue Omaha, NE 68114


*Solutionary is the proud winner  
of these prestigious industry  
awards for our ActiveGuard®  
and SecurCompass® offerings.*




 [www.solutionary.com](http://www.solutionary.com)

 [info@solutionary.com](mailto:info@solutionary.com)

 +1 402.361.3000

 +1 866.333.2133

 +1 402.361.3100

2. Successful completion of an **annual security assessment**, which may be either a self-assessment questionnaire (SAQ) or an on-site assessment conducted by a certified vendor such as Solutionary, depending on your level.

**Requirements by level:**

MERCHANT LEVEL	MERCHANT DEFINITION	COMPLIANCE
Level 1	More than six million V/MC transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 - 5,999,999 V/MC transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 3	20,000 - 1,000,000 V/MC e-commerce transactions annually	Annual Self-Assessment and Quarterly Network Scans
Level 4	Less than 20,000 V/MC e-commerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self-Assessment and Annual Network Scans

SERVICE PROVIDER LEVEL	SERVICE PROVIDER DEFINITION	COMPLIANCE
Level 1	All VisaNet processors (member and Nonmember) and all payment gateways.*	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 V/MC accounts/transactions annually	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 V/MC accounts/transactions annually.	Annual Self-Assessment Questionnaire and Quarterly Network Scans

**Q: What can I do on my own?**

**A:** That depends on the level of merchant that you are. As seen in the tables, Level 2-4 Merchants can do the annual SAQ using internal resources; however no matter which level you are, however, you must have a qualified third-party vendor (such as Solutionary) do the vulnerability scanning.

**GET COMPLIANT. STAY COMPLIANT.**

**Q: What is the Solutionary PCI compliance program?**

**A:** Solutionary offers comprehensive and easy-to-use services that accelerate and simplify the process of attaining and maintaining PCI compliance.

**Q: What are the key elements of the Solutionary PCI compliance program?**

**A:** Solutionary’s PCI Compliance program is a diverse solution that demonstrates a complete understanding of the PCI DSS.

► **PCI Quarterly Vulnerability Scans**

Solutionary uses certified best-of-breed vulnerability assessment tools and processes to attain and maintain certified results for ensuring compliance with the PCI standard’s Quarterly Vulnerability Scanning requirements. Utilizing PCI-certified scanning utilities and methodologies for each merchant, Solutionary detects, identifies and reports vulnerabilities common to flawed web site architectures, configurations and Internet-facing system components. These vulnerabilities, if not remedied in PCI system components, could lead to an unauthorized intrusion or theft of cardholder data.

**Solutionary, Inc.** 9420 Underwood Avenue Omaha, NE 68114

*Solutionary is the proud winner of these prestigious industry awards for our ActiveGuard® and SecurCompass® offerings.*



By proactively identifying and providing the opportunity to remedy such vulnerabilities on Internet-facing system components, PCI-compliant products and services offer a means for reducing risk of intrusion and data compromise. These assessments are run on a quarterly basis, and results are documented in quarterly reports.

► **PCI Annual On-Site Assessments**

Solutionary also offers PCI Annual On-Site Assessments for merchants and their Internet-facing system components. Solutionary takes the extra step of assessing the individual Findings for each system component by assigning relevant fix actions that will aid in gaining or maintaining compliance.

Findings for each system are listed, and an overall compliance rating is assigned for each system component. Solutionary includes a prioritized action plan for all Findings that need to be addressed before compliance can be attained, as well as individual matrices for each assessed system.

The **Solutionary PCI Compliance Assessment Report** is the merchant's roadmap for compliance. With separate sections for executive and technical audiences, this report is customized to your needs and is easily understood at every audience level.

► **PCI Managed Services**

Deploying, maintaining and securing the systems required by the PCI Data Security Standard requires specialized expertise, continuous monitoring and comprehensive management to keep all of the system components operating at peak performance. Proper security management is a resource-intensive activity that most merchant organizations cannot afford due to the expertise, budget and time required. Solutionary' managed security services expertise relieves merchants of these burdens by performing all activities required for PCI compliance. These end-to-end compliance management services are merged into one comprehensive security intelligence solution tailored to each merchant's risk profile and unique security posture.

Please contact Solutionary for the complete mapping detail of our services to the specific PCI DSS regulations.

**Q: What technology does Solutionary use?**

**A:** Solutionary uses PCI-certified, best-of-breed technologies including application scanners and proprietary processes, all as approved by the PCI Council, and as relates to your organization's needs for professional security assistance.

**Q: What if the scan result shows that my site has vulnerabilities?**

**A:** Solutionary has the experts, processes, and technologies to identify and help remediate vulnerabilities of failed system components before the compliance deadline.

**Q: What happens after my systems have been scanned and my company has completed the security assessment?**

**A:** Solutionary includes a prioritized action plan for all Findings that need to be addressed before compliance can be attained, as well as individual matrices for each assessed system.

**Q: What happens if I don't pass the tests for PCI compliance?**

**A:** Solutionary will work with you to get compliant with all the requirements of the PCI standard.

**Solutionary, Inc.** 9420 Underwood Avenue Omaha, NE 68114

*Solutionary is the proud winner of these prestigious industry awards for our ActiveGuard® and SecurCompass® offerings.*



**Q: Does Solutionary provide customer support as part of its PCI compliance services?**

**A:** Absolutely! Solutionary provides a dedicated PCI compliance program account manager and Solutionary is the only vendor to be there with you each month, each quarter, and whenever you need us. Solutionary will be there with you to ensure ultimate mitigation for vulnerabilities – and to help you attain and maintain compliance. We help you get compliant We help you stay compliant.

**Q: How do I get started?**

**A:** Call us at 866.333.2133 or email us at [info@solutionary.com](mailto:info@solutionary.com).

**Q: What if I have already paid for compliance from another PCI security company?**

**A:** If you are already using another PCI compliance service, you can easily switch to Solutionary and realize significant savings while improving your company's overall security posture.

**Q: Who is Solutionary?**

**A:** Solutionary is a PCI-approved vendor (one of the original ten) that has successfully completed the rigorous compliance testing process required by the PCI Council in order to perform scans, assessments, and audits.

Moreover, Solutionary is the leader in managed security solutions that leverage clients' existing security resources and previous investments in technology. Offering well-defined service level agreements (SLAs), Solutionary provides expert customization, as well as real-time monitoring and response to improve all aspects of an enterprise's Information System security posture. Solutionary enables organizations to improve the speed, efficiency and effectiveness of their systems security, thereby reducing operational costs, mitigating digital risks and promoting compliance with standards and regulations including PCI DSS, CobiT, SOX, ISO, GLBA, HIPAA, S.B. 1386, etc.

**Q: Where can I find card-issuer information about the PCI requirements?**

**A:** Visit the PCI Council at <https://www.pcisecuritystandards.org/>


**Solutionary, Inc.** 9420 Underwood Avenue Omaha, NE 68114


*Solutionary is the proud winner of these prestigious industry awards for our ActiveGuard® and SecurCompass® offerings.*




 [www.solutionary.com](http://www.solutionary.com)

 [info@solutionary.com](mailto:info@solutionary.com)

 +1 402.361.3000

 +1 866.333.2133

 +1 402.361.3100