



Payment Card Industry (PCI) Standards and Compliance

Tips and Techniques for Success

igxglobal, Inc.
Threat Mitigation Division
January 15, 2010
Version 1.3

PCI INFORMATION YOU NEED TO KNOW

Background

Identity theft is a crime that impacts consumers, retail merchants, and financial institutions worldwide. Just last year, consumers in the United States filed over 685,00 complaints of identity theft and consumer fraud and reported losses of more than \$680 million¹. This pushes the total to over 100 million identities compromised in the last two years.

To address this alarming trend, the major payment card companies - including Visa International, MasterCard Worldwide, American Express, JCB, and Discover Financial Services – created standards to prevent theft of consumers' data. In September 2006, they jointly announced the formation of the Payment Card Industry Security Standards Council (PCI SSC) and released the PCI Data Security Standard (PCI DSS).

What is PCI Compliance?

PCI compliance involves fulfilling the PCI Data Security Standard (PCI DSS) and also adhering to requirements defined by the individual payment card companies. The PCI DSS is a multi-faceted security standard that includes requirements such as security management, policies, procedures, network architecture, and software design. It also includes validation regulations that require specific auditing procedures.

Note that the PCI Data Security Standard and associated compliance standards are not laws – they are contractual obligations with the credit card companies. Thus, while the PCI Security Standards Council manages the underlying Data Security Standard, compliance requirements are actually set independently by individual payment card companies. Requirements and stipulations for compliance validation may vary slightly, depending on the payment card company.

Who Must Demonstrate PCI Compliance?

PCI compliance is required for all organizations that collect, store or transmit payment card account data. This includes retail and wholesale merchants, point-of-sale (POS) vendors, payment account processors, and financial institutions using credit/debit or paycard data.

What Are the Penalties of Non-Compliance?

Payment card companies may enforce the terms of their contracts by imposing fines and/or sanctions. For example, a non-compliant organization can be barred from processing card transactions, be subject to higher processing fees, and if a serious breach occurs, be fined up to \$500,000 for each non-compliance instance.

While non-compliance penalties vary among the major payment card companies, they can be substantial. Visa fined 77 organizations for a total of \$4.7 million in its fiscal 2006⁵. In October 2006, MasterCard and Visa began fining for storing magnetic stripe data in violation of the PCI standard - when no data compromise had yet occurred. Within seven months these fines can escalate from \$10,000/month to \$100,000/month⁶.

What Are the Benefits of PCI Compliance?

The benefits of PCI compliance are three-fold. First, demonstrated compliance with the PCI standards provides “safe harbor”, which protects organizations from fines and sanctions in the event that a breach occurs. (Note, however, that this protection is not applicable if the organization has not fulfilled all compliance requirements at the time of the breach). Second, initiatives designed to achieve PCI compliance can be integrated with other relevant regulations, such as HIPAA, GLBA, CALEA, and state privacy or disclosure laws). Third, since many PCI compliance requirements are fundamental to information security, compliance may help protect your reputation, gain competitive advantage, increase revenue and improve the bottom line, and generate continued confidence in the payment card industry.

HOW PCI COMPLIANCE WORKS

PCI DSS Requirements

The Payment Card Data Security Standards (PCI DSS) defines twelve (12) requirements for compliance, organized into six (6) categories. Your organization must address and document its compliance with each of the twelve requirements, listed below:

PCI DSS Categories	PCI DSS Requirements
Build and Maintain a Secure Network	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ Requirement #3: Protect stored data ▶ Requirement #4: Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> ▶ Requirement #5: Use and regularly update anti-virus software ▶ Requirement #6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ Requirement #12: Maintain a policy that addresses information security

Validation of PCI Compliance

Validation of PCI compliance is distinct from actually achieving compliance with the PCI DSS. Specifically, validation involves *demonstrating* PCI compliance using a stringent and systematic methodology.

To provide a uniform approach to account data protection world-wide, the PCI Security Standards Council has developed a “levels” approach. The levels for PCI compliance validation are based on each organization’s volume of transactions, potential risk, and exposure introduced to the payment card industry.

Merchants are categorized according to one of four levels as follows²:

Level	Description of Merchant Level
1	<ul style="list-style-type: none"> ▶ Processing over 6,000,000 transactions per year – regardless of acceptance channel ▶ Has suffered a hack or an attack that resulted in an account data compromise ▶ Identified by a payment card company as Level 1
2	▶ Processing 1,000,000 to 6,000,000 transactions per year – regardless of acceptance channel
3	▶ Processing 20,000 to 1,000,000 e-commerce transactions per year
4	<ul style="list-style-type: none"> ▶ Processing fewer than 20,000 e-commerce transactions per year ▶ Processing up to 1,000,000 Visa transactions per year - regardless of acceptance channel

Service Providers are categorized into one of three levels as follows:

Level	Description of Service Provider Level
1	Any card processor (member and nonmember) and all payment gateways
2	Any Service Provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 card accounts or transactions annually
3	Any Service Provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 card accounts or transactions annually

VALIDATING YOUR PCI COMPLIANCE

The Two Components

Validation of PCI compliance involves two components: 1) an annual security assessment; and 2) quarterly network security scans. The annual security assessment may be an on-site or self-administered review, depending on the organization's assigned level. The network scan uses an automated tool that checks systems for vulnerabilities by conducting a non-intrusive scan to remotely review networks and Web applications based in the externally-facing Internet Protocol (IP) address provided by the merchant. Since the PCI standard refers to all areas of data security, all relevant applications - not merely EFT software - must be considered when assessing compliance.

Impact of Levels

Specific requirements for validation depend on each organization's level. For example, Level 1 merchants must complete an Annual Onsite PCI Data Security Assessment, conducted in accordance with the PCI Audit Procedures, and a Quarterly Network Security Scan. Level 2 and Level 3 merchants must complete the Annual Self-Assessment Questionnaire as well as a Quarterly Network Security Scan. Level 4 merchants may be required to complete the Annual Self-Assessment Questionnaire plus the Quarterly Network Security Scan.

The following chart summarizes the validation requirements for each level:

Level	Validation Action	Validated By
1	<ul style="list-style-type: none"> ▶ Annual On-Site PCI Data Security Assessment AND ▶ Quarterly Network Scan 	<ul style="list-style-type: none"> ▶ Qualified Security Assessor or Internal Audit, if signed by Officer of the organization ▶ Approved Scanning Vendor
2	<ul style="list-style-type: none"> ▶ Annual PCI Self-Assessment Questionnaire AND ▶ Quarterly Network Scan 	<ul style="list-style-type: none"> ▶ Merchant ▶ Approved Scanning Vendor
3	<ul style="list-style-type: none"> ▶ Annual PCI Self-Assessment Questionnaire AND ▶ Quarterly Network Scan 	<ul style="list-style-type: none"> ▶ Merchant ▶ Approved Scanning Vendor
4*	<ul style="list-style-type: none"> ▶ Annual PCI Self-Assessment Questionnaire AND ▶ Quarterly Network Scan 	<ul style="list-style-type: none"> ▶ Merchant ▶ Approved Scanning Vendor

**The PCI DDS requires that all merchants perform external network scanning to achieve compliance. Acquirers may require submission of scan reports and/or questionnaires by Level 4 merchants.*

Using Certified Providers to Validate PCI Compliance

Certain validation components must be completed by a company certified by the PCI Security Standards Council. Specifically, Qualified Security Assessors (QSAs) provide organizations with their onsite security assessments, strictly adhering to the PCI Audit Procedures that are defined in the PCI DSS. Based on this security assessment, they then complete the Report on Compliance. Approved Scanning Vendors (ASVs) must complete organizations' Quarterly Network Scans.

Validation of PCI compliance takes place at the organization's expense. Cost depends on the volume of card transactions and the scope of the assessment. The cost of any remediation services is dependent on a pre-compliance review and/or on-site audit and, therefore, will be specific to individual organizations.

The Importance of Monitoring

Compliance validation requirements and enforcement measures are subject to change, so your organization should closely monitor the requirements of all payment card providers in which you are involved.

YOUR NEXT STEPS TO ACHIEVING PCI COMPLIANCE

To achieve PCI compliance, you need to start with the following four key steps:

#1. Understand your PCI compliance requirements

- ▶ Identify your organization's level and the associated compliance requirements
- ▶ Pinpoint the overlap between your PCI compliance requirements and other relevant regulations (e.g., HIPAA, GLBA, state privacy/disclosure laws, CALEA)
- ▶ Review best practices of the PCI Council, payment card companies, and industry specialists
- ▶ Develop the business case and necessary budget. Leverage PCI compliance requirements to address your organization's other key information security issues and risks

#2. Conduct a self-assessment

- ▶ Identify the appropriate scope of assessment. The self-assessment should be holistic and proactive, and it may not need to encompass the entire organization
- ▶ Use a gap analysis approach to understand the discrepancies between your organization's current state and its PCI requirements.
- ▶ Consider hiring a PCI-certified security consulting company for assistance. The self-assessment forms are relatively complex and most organizations do not have the bandwidth to evaluate compliance. Also, an assessor will eventually be required for validation of PCI compliance, so it may be preferable to bring the assessor in early as an advocate than later as a watchdog

#3. Address key issues

- ▶ Set, communicate, and document your policies
- ▶ Focus on training, monitoring and enforcement, not just technology
- ▶ Implement your technology solutions

#4. Schedule and complete your assessment and quarterly scans

- ▶ Define an assessment schedule
- ▶ Select an assessment vendor. Solicit proposals from at least three QSAs. Ensure that you request at least two references of prior PCI assessments and find out the level of support the QSA can provide after the assessment
- ▶ Complete the assessment and remediate as needed

Deadlines for demonstrating PCI compliance have already passed for Level 1 and Level 3 merchants. Newly classified Level 2 merchants have until September 30, 2007 to demonstrate compliance. Most Level 3 and Level 4 merchants will probably continue to fly under the radar until the payment card companies have categorized the more than 3,000 Level 3 and approximately 6 million Level 4 merchants.

Tips for PCI Compliance

We find that many organizations experience the following "real-life" compliance issues:

- | | |
|--|--------------------------------------|
| ▶ Merged networks | ▶ Information leakage |
| ▶ Lack of encryption | ▶ Loss of tapes or laptops |
| ▶ Storing of track data | ▶ Weak or un-enforced policies |
| ▶ Lack of knowledge about location of data | ▶ Insufficient monitoring |
| ▶ Lack of strong access controls | ▶ Little to no auditing capabilities |

HOW IGXGLOBAL CAN HELP YOU ACHIEVE PCI COMPLIANCE

igxglobal is certified by the PCI Security Standards Council as a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV). We have provided more than one hundred fifty (150) security assessments and Quarterly Network Scans over the past three years to U.S.-based and international organizations of all sizes. Since igxglobal has an international presence, we can provide PCI compliance assistance to your organization's offices across the world.

Our certified QSAs can provide an onsite security assessment, strictly adhering to the PCI Audit Procedures that are defined in the PCI DSS, and complete the Report on Compliance. As an Approved Scanning Vendor (ASV), we are certified to complete the required Quarterly Network Scans.

igxglobal provides the following PCI-related services:

- ▶ PCI DSS GAP Analysis and Compliance Accreditation
- ▶ Quarterly external and internal vulnerability scans
- ▶ Annual penetration testing
- ▶ Email compliance audits
- ▶ Source code review and Application assessments
- ▶ Privacy data identification and location analysis
- ▶ Wireless analysis and site mappings.

PCI Audit and Assessment

The igxglobal **PCI Audit and Assessment** includes the following items:

- | | |
|---|---|
| ▶ Policy and Procedure Review | ▶ Wireless Network Security Analysis |
| ▶ System Inventory & Documentation Collection | ▶ Active Social Engineering |
| ▶ PCI Data Flow Analysis | ▶ Third Party Oversight Review |
| ▶ Internal Vulnerability Assessment | ▶ Physical/Environmental Security Review |
| ▶ Host/Network Diagnostic Review | ▶ Personnel and IT Staff Training and Awareness |
| ▶ Access Control Review | ▶ Testing of Deployed Security Measures |
| ▶ Network Usage Analysis | ▶ Monitoring/Response Process Assessment |

Upon completion of the PCI Audit and Assessment, two reports are provided. The first report is a formal submission to the Payment Card industry conveying the organization's current compliance state, called the Report on Compliance (ROC). The second report to our clients provides copies of notes, raw data and logs collected during the assessment to prioritized recommendations for remediation.

We Are Here To Help

We will provide a one-hour conference call with you and one of our QSA/Compliance specialists to discuss your current PCI/regulatory compliance status, determine if any other regulations apply to you, identify which regulations are being violated, and determine how best to establish PCI compliance.

LEARN MORE

A range of free information about PCI compliance is available, including:

- ▶ PCI Standards Council homepage (<https://www.pcisecuritystandards.org>)
- ▶ Visa Cardholder Information Security Program – United States (www.visa.com/cisp)
- ▶ Visa Account Information Security Program – Europe (<http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp>)
- ▶ List of PCI-Accredited Vendors (https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf)
- ▶ Answers to Common Questions About PCI Compliance (<http://www.gartner.com>)
- ▶ Enterprise Compliance Solutions for the Payment Card Industry (<http://www.verisign.com>)
- ▶ Identity Theft Information and Rates – United States (<http://www.ustreas.gov>)
- ▶ Fraud Prevention – United Kingdom (<http://www.cifas.org.uk>)
- ▶ Fraud Prevention – South Africa (<http://www.safps.org.za>)
- ▶ A Chronology of Data Breaches (<http://www.privacyrights.org/ar/ChronDataBreaches.htm>)

Also, keep an eye out for upcoming **igxglobal** PCI Compliance newsletters:

- ▶ Dos and Don'ts in PCI Compliance
- ▶ Maximizing your Returns on PCI investments
- ▶ Preparing for the 2008 PCI Application Security Requirements

References

- ¹ Consumer Sentinel (complaint database developed and managed by the Federal Trade Commission; <http://www.consumer.gov/sentinel/trends.htm>)
- ² CIFAS Online (http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp)
- ³ SC Magazine, "Four Million UK Users hit by Identity Theft" (<http://www.scmagazine.com.au/news/43463,four-million-uk-users-hit-by-id-theft.aspx>)
- ⁴ United States Department of the Treasury (www.treas.gov/press/releases/js3087.htm)
- ^{5,6} Gartner's Answers to Common Questions About PCI Compliance (http://www.gartner.com/DisplayDocument?doc_cd=144907)
- ⁷ PCI Standards Council homepage (<https://www.pcisecuritystandards.org>)
- ⁸ Visa Cardholder Information Security Program (www.visa.com/cisp)

ABOUT IGXGLOBAL

Our Mission

igxglobal provides information technology services and solutions designed to improve the performance, infrastructure and security of our clients' operations.





At igxglobal, we are committed to helping our customers operate their networks with more security, efficiency and reliability. We pledge to understand your business model, your customers, and your expectations in order to provide you with the most viable information technology solution.

With a customer focused approach and a comprehensive life cycle model of solutions, we will be your long term partners in ensuring the performance, infrastructure and security of your information networks.

Services and Solutions

igxglobal's services and solutions provide our clients with: risk analyses to pinpoint and address vulnerabilities and threats; assessments and audits to ensure compliance with regulations; tools to improve performance and strengthen infrastructure; subject matter experts to provide technical expertise and impartial advice; specialists to resource short term services or long term deployments; and information security intelligence to sustain our clients' infrastructure investments.

These solutions are systematically delivered in our core practice areas:

-  Threat Mitigation Services
-  Information Technologies
-  Professional Services
-  Security Operations Services

Whether your requirements warrant strategic or operational solutions, or the implementation is handled by your resources or ours, igxglobal has the experience, expertise and knowledge to enhance your networks performance, infrastructure and security.

Corporate Headquarters

50 Inwood Road
Rocky Hill, CT 06067
860.513.0112
888.393.4449
info@igxglobal.com

Threat Mitigation Division

5710 Ogeechee Road
Suite 200-304
Savannah, GA 31405
912.220-6664
888.393.4449

Metro NJ & NYC Sales and Professional Services

100 Delawanna Avenue
Clifton, NJ 07601
201.498.0555
888.393.4449

UK-EMEA Operations igxglobal Ltd

33 Throgmorton Street
Bank, London EC2N 2BR
United Kingdom
+44.0.207.156.5065