IBM Internet Security Systems
Ahead of the threat.™

The Payment Card Industry Data Security Standard How and Why to Become Compliant

By Howard E. Glavin Jr.

Principle Consultant and Manager of Governance Services for
IBM Internet Security Systems

Table of Contents

Purpose

Companies that store or process payment card information need to understand the Payment Card Industry (PCI) Data Security Standard and why compliance with the standard is in their best interests. American Express, Discover, Diners Club and JCB have also adopted the PCI standard, extending it beyond Visa and MasterCard. This whitepaper will explain PCI requirements, the benefits of compliance and the potential issues for failing to comply.

Background

The history of PCI data security requirements mirrors most other regulations and requirements in the financial services industry. Past problems and data losses pressured the industry and the government to require safeguards to protect the credit card data being stored.

Resulting from the combined efforts of Visa and MasterCard, the PCI Data Security Standard has created common industry requirements for safeguarding cardholder data. Other credit card brands – including American Express, Discover, Diners Club and JCB – have since adopted the standard as well.

The PCI standard started with Visa’s Cardholder Information Security Program (CISP program) in 1999 for e-Merchant certification. The PCI standard aligns Visa’s CISP program with MasterCard’s Site Data Protection (SDP) program. When the PCI Data Security Standard was developed in 2003, the CISP program was rolled into the new standard.

In September 2006, the PCI Security Standards Council (PCI SSC) was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. This new organization makes the PCI Data Security Standard a global standard across all of the participating card brands. The PCI SSC was formed to "develop, enhance, disseminate and assist with implementation of security standards for payment account security."

This body is responsible for the management and evolution of the PCI Data Security Standard, but not compliance. Compliance validation requirements and processes I remain a function of the individual payment card brand's compliance programs (i.e. Visa USA's CISP and MasterCard's SDP programs). The individual payment card brands may institute additional requirements as part of their compliance programs. The individual card brands are also responsible for determining which entities must be compliant. Additionally, they are responsible for any brand-specific enforcement programs.

As Visa USA's CISP standard is the basis for much of PCI SSC, this whitepaper focuses on the Visa USA requirements, although there are slight variations in the requirements for the other five Visa regions.

The Security Audit Procedures version 1.1, dated September 2006, enumerates the current PCI standard from an audit perspective. The PCI DSS is A good background document for the requirements for compliance, the Security Audit Procedures can be found on the PCI Security Standards Council Web site at www.pcisecuritystandards.org.

Do PCI Requirements Apply to My Business?

As with all regulatory and business requirements, the first step in the process is understanding whether the requirements apply in the first place. Visa and MasterCard, along with several other credit card brands, apply varying PCI requirements based on the type of business conducted and transaction volume. Businesses are categorized as merchants, service providers and gateways.

Merchants

The merchant is the store, company or location that accepts credit cards as payment for goods or services (specifically credit cards issued by Visa, MasterCard, American Express, Discover, Diners Club and JCB).

Merchants must be PCI compliant if the credit cards they accept can be used at locations other than their store. Some merchants issue a proprietary card that is only to be used at their locations and will not accept any other form of credit card. These locations do not require PCI certification as they are self contained and are fully responsible for their line of business. If the store accepts its proprietary card and those form other vendors like Visa and MasterCard then they are required to be compliant.

PCI requirements divide merchants into four different levels. Visa updated the merchant validation levels for the PCI Data Security Standard in a July 18, 2006 CISP bulletin. The updated levels appear below:

> MERCHANT LEVEL 1
> Merchants that process more than six million Visa or MasterCard transactions per year, or who are classified as a Level 1 by any other payment card brand. Each time a card is accepted for goods or services or as payment, it is considered a transaction. Additionally, merchants that have experienced a data security breach or a successful online attack in the past year are considered a Level 1 Merchant, regardless of transaction volume.

MERCHANT LEVEL 2
Level 2 Merchants process one to six million credit card transactions per year.

MERCHANT LEVEL 3
Level 3 Merchants process 20,000 to one million e-commerce transactions per year.

MERCHANT LEVEL 4
Level 4 Merchants include those processing less than 20,000 e-commerce transactions per year, and all other merchants processing up to one million credit card transactions each year.

Transaction volumes sited above are based on merchants "Doing Business As" (DBA), not on a corporation that has several DBAs as part of its structure.

Service Providers

Service providers are companies that contract their services with a merchant or bank to handle credit card transactions on their behalf. Visa currently defines three levels of service providers.

SERVICE PROVIDER LEVEL 1
Level 1 service providers are all companies that connect directly to the VisaNet (Visa members and non members) and payment gateways.

SERVICE PROVIDER LEVEL 2
All service providers that are not a Level 1 and store, process, or transmit more than one million account transactions annually.

SERVICE PROVIDER LEVEL 3
Any service provider that is not a Level 1 and stores, processes, or transmits less than one million transactions annually.

Gateways

Gateways are a category of service provider that enables payment transactions between merchants and processors. Merchants may send transactions directly to an endpoint or send them indirectly through a gateway. Also known as "payment gateways," these companies are simply the pipe for the transactions to flow through and have no interaction with the actual transaction other than providing this service.

The PCI Data Security Standard

The PCI Data Security Standard consists of 12 areas of best practices that are organized into six primary categories. Each of the best practice areas contains detailed sub-requirements.

The six categories of PCI standard best practices include:

1. Build and Maintain a Secure Network
   - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
   - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Card Holder Data
   - Requirement 3: Protect stored cardholder data
   - Requirement 4: Encrypt transmission of cardholder data across open, public networks

3. Maintain a Vulnerability Management Program
   - Requirement 5: Use and regularly update anti-virus software
   - Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures
   - Requirement 7: Restrict access to cardholder 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

5. Regularly Monitor and Test Networks
   - Requirement 10: Track and monitor all access to network resources and cardholder data
   - Requirement 11: Regularly test security systems and processes

6. Maintain an Information Security Policy
   - Requirement 12: Maintain a policy that addresses information security

Although they appear fairly simple, these standards require a sufficient number of checkpoints for detailed evaluations of a company's protection of cardholder data. These standards also validate that a company is not keeping any data that it is not entitled to keep under the PCI requirements. Examples of data that cannot be retained after the authorization is granted include:

- CVV2
- CVC
- PIN
- Full Track Data for Track One
- Full Track Data for Track Two

The evaluation for retained data applies to all potential areas of the data stream to validate that only the required data is maintained and that all other data is removed and wiped by a Department of Defense (DoD) approved process if it were written to any media other than volatile memory. Some of these areas of the data stream include:

- Databases
- Backup files
- Transaction logs
- Access logs
- Application logs
- Device logs
- Error logs and reports
- Core and memory dumps used for diagnostic purposes

Production Cardholder Data Use in Testing

One of the common errors discovered in the PCI audit process is the use of production data in the test region. The use of production cardholder data in testing is expressly prohibited by the PCI standard.

Fictitious data should be employed for testing to ensure that the testing data does not place the production data at risk and put the company out of compliance as a result of using actual cardholder data for testing purposes.

Simply moving the main fields around does not render the data usable as the protected entity is the full credit card account number. If the full credit card number used in testing is an actual credit card number from the production region, the company is out of compliance regardless of the compensating controls used during the testing.

Labeling Cardholder-related Media as Confidential

Labeling cardholder data with a data classification of "confidential" (or whatever classification the company employs to indicate its most protect assets) becomes another potential issue. Security by obscurity is not acceptable. The labels must be affixed to both the physical media and electronically shown on the media.

Encryption Requirements

The PCI data standard requires that the full card number be rendered unreadable anywhere it is stored. Encryption is recommended as an accepted and effective means to secure data, but is not the only approach for PCI compliance. Compensating controls that meet the intention and rigor of the PCI requirement can be an alternative to encryption if encryption can not be used.

Encryption of the full credit card number using a commercial-based algorithm that is a minimum of 3DES bit length of 128 or AES of 256 bit length is recommended for all storage of cardholder data.

The Report on Compliance (ROC)

The ROC is a simple method for documenting the critical areas of data management, in accordance with PCI requirements. The ROC is generated upon the successful completion of a PCI assessment.

Submission of the Report on Compliance (ROC)

The individual card brands (i.e. Visa) are responsible, under PCI SSC, for reviewing and approving ROCs according to their own compliance programs and procedures. Visa requires that the ROC is submitted to one of two entities:

1. The Acquirer Bank if the company is a Merchant
2. To Visa if the company uses Visa Net or is a service Provider.

Upon receipt, Visa will certify that it accepts the ROC and will then post the company's name as having passed the annual ROC audit.

The company is now compliant for a period of one year from the date of the accepted ROC.

Submission via an Acquirer Bank

As a rule of thumb, if the company is associated with Visa through an acquirer bank then the ROC goes to the acquirer bank for acceptance and is then forwarded by them to Visa. If the company is part of Visa Net or designated by Visa for submission to Visa, then the report goes directly to Visa for its acceptance.

In both cases Visa has the right and obligation to review the report and ask clarifying questions to determine if it will in certify the company as PCI compliant.

Additionally the company and the third-party assessor must certify to the acquirer bank or Visa that the facts represented in the ROC are true and correct entries. Additionally, the certification states that only the PCI-permitted cardholder data is retained for the limited time required for business protection.

Submission of a ROC with a “Not in Place” entry in the ROC Report

In the past, Visa would accept the ROC with entries marked “Not in Place” when accompanied by an action plan stating when the entry could change to “In Place.” This acceptance has changed. Visa now requires all line entries and each numbered or bulleted item to be discussed in the comments area. The entry must be marked by the assessor as “In Place.” This acceptance holds for all ROCs, whether they are sent to the acquirer or to Visa.

Submission of a ROC with all Areas Marked as “In Place.” Now What?

Whether submitting directly to Visa or to an acquiring bank, companies must also submit a certification of accuracy to the same company to whom it submitted the ROC.

When Visa accepts the ROC, the company will be notified of its acceptance. Note that the report may be dated in January and accepted in May. The time for the next annual submission will be January.

If the ROC is submitted to the acquirer, the acquirer must review it, accept it (or request clarification) and submit it to Visa. This process may take longer than submitting directly to Visa. As with the Visa direct submission, the time for the next ROC is the date plus one year or upon a substantial change to the company’s environment, whichever comes first.

The acquirer or Visa can reject the submission and request the company to rework it and correct deficiencies. Generally speaking, these rejections center around the storage of data not permitted and compensating controls.

What Does all this Mean to the Company?

The compliance requirements vary by level for Merchants and Service Providers. The intent of the "levels" is to allow for varied degrees of determining PCI compliance. In short, all Level 1 companies and most Level 2 companies are required to have third parties conduct part or all of the PCI audits.

The tables below outline the validation requirements by level.

PCI Data Security Standard for Merchants by Level

Merchant Level	Validation Action	Validated By
Level 1	• Annual on-site PCI Data Security Assessment • Quarterly network scan	• Qualified Data Security Company or internal audit if signed by officer of the company • Qualified Independent Scan Vendor
Level 2	• Annual PCI self-assessment questionnaire • Quarterly network scan	• Merchant • Qualified Independent Scan Vendor
Level 3	• Annual PCI self-assessment questionnaire • Quarterly network scan	• Merchant • Qualified Independent Scan Vendor
Level 4	• Annual PCI self-assessment questionnaire • Quarterly network scan Annual PCI self-assessment questionnaire	• Merchant • Qualified Independent Scan Vendor

The full definition for the levels is available on the Visa CISP Web site at: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html

PCI Data Security Standard for Service Providers by Level

Merchant Level	Validation Action	Validated By
Level 1	• Annual on-site PCI Data Security Assessment • Quarterly network scan	• Qualified Data Security Company • Qualified Independent Scan Vendor
Level 2	• Annual on-site PCI Data Security Assessment • Quarterly network scan	• Qualified Data Security Company • Qualified Independent Scan Vendor
Level 3	• Annual PCI self-assessment questionnaire • Quarterly network scan	• Service Provider • Qualified Independent Scan Vendor

The full definition for the levels is available on the Visa CISP Web site at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html.

As these requirements change from time to time, the Visa Web site should be checked periodically to get the latest updates to the full audit requirements and the need for third-party validation.

How Do Companies Become Compliant?

The most efficient method for compliance is to practice safe data management, based on the Visa requirements, underpinned by following a best practices framework such as ISO 17799.

Following a best practices framework helps ensure that security initiatives are coordinated with business processes. This can aid compliance with multiple regulations (such as HIPAA, Sarbanes-Oxley and Gramm Leach Bliley) as many of the business processes outlined in the framework map back to multiple regulations. If business processes are not aligned with security initiatives, there is a high likelihood that the initiative will fail.

Choosing a Third Party Vendor When a PCI Audit, Scan or Penetration Test is Required

The PCI Security Standards Council has an approved list of vendors that can conduct each audit phase. Companies can conduct their own penetration testing (although this can also be outsourced).

A third party company is required to conduct the quarterly scans, if the level indicates this need. The actual ROC can be completed by a third party certified vendor or by an internal audit group, depending on the company's level.

Most certified assessors, like IBM Internet Security Systems (ISS), can conduct all parts of the audit process. This can also be broken down to just the parts a company chooses to outsource, either as the result of the level or the expectations the company has for a third party review.

Effective December 1, 2006, the PCI SSC began management of the Qualified Security Assessor (QSA) program and the Approved Scanning Vendor (ASV) program. The PCI SSC maintains a list of certified assessors at http://www.pcisecuritystandards.org.

Choosing a Vendor

Choosing a vendor to assist is critical to the full assessment process. Level 2 and 3 companies are permitted to complete the ROC based on a self assessment. Level 1 companies are required to use a third party vendor to complete the ROC.

- Only approved and certified companies and assessors are permitted to conduct third-party ROC assessments.

- Choose a vendor that is capable of supporting the pre-assessment through the completion and submission of the final ROC.

- A vendor should offer alternative methods for achieving the same level of protection and should assist with the definition of the remediation and mitigation tasks that may be required. Generally speaking, the work effort, from the first efforts of the pre-assessment to the final submitted ROC, may take two to eight months, depending on company size and the number of “not in place” items uncovered.

- The vendor is the company's advocate. The vendor chosen should be a trusted security advisor. The vendor will be the one working with the PCI SSC, the card brand or the acquirer on the company's behalf.

- The vendor should have expertise in the company's industry to ensure it receives cost-effective remediation activities, not just a recommendation to become compliant.

- Choose a vendor that is security-focused. Many vendors may offer compliance services, but vendors that have security as a core competence are better-suited to addressing overall security posture and making recommendations for securing the infrastructure.

PCI Assessments are like custom-made clothing. If conducted correctly, they fit the company's needs and meet all the requirements for the PCI protection standards. Some assessing third party vendors offer discount prices, but a bargain-rate firm may not be able to support the company's unique needs.

Companies should also examine what they receive for their investment. Are they getting the benefit of expert security expertise or merely the output of an automated vulnerability scan? In many cases, contracts for PCI assessments are multi-year contracts, so understanding the services companies will and will not receive is imperative.

Companies need to approach the choice of PCI assessment partner like any other critical business decision. They should look for depth and capabilities in the vendor. The vendor is the company's advocate, so they should choose a partner that will be a long-term resource. Other important factors include consultant experience, the number of PCI audits they have conducted and how many of their reports on compliance have been accepted by the card brand or the acquirer.

Companies need to have a firm understanding up front of what they will receive, when they will receive it and in what format will it be delivered. Will the vendor provide an upfront assessment to determine what remediation efforts the company will need to undertake? Will the vendor supply detailed recommendations? Lastly, will the vendor supply the ROC and letter of compliance?

Benefits of Compliance

Media coverage of security breaches and identity theft have placed a spotlight on the payment industry. Demonstrating a proactive approach to the safeguarding of customer data helps companies, and the industry as a whole, build a culture of security that benefits everyone.

Visa recognizes the potential benefits of compliance listed in the table below:

Compliance Benefits	
Everyone	• Reduce risk • Increase confidence in payment industry
Members	• Protect reputation
Merchants and Service Providers	• Gain competitive edge • Increase revenue and improve bottom line • Maintain positive image • Protect customers
Industry	• Encourage “good security neighbors”
Consumers	• Safeguarding of information • Prevention of identity theft

Cardholder Data Loss for Compliant Companies

Companies that are compliant at the time of the loss, and previously certified as ROC compliant, are put into the Visa “Safe Harbor” process. Compliance will be validated during the forensics examination stage of the investigation, so any stance other than full compliance will be documented and noted as non compliance.

Companies with an approved ROC that fail to maintain the same degree of care, custody and control as required by the PCI data security standards are considered non-compliant and therefore subject to the “the fines and cost” cited below.

A Safe Harbor finding by the Visa approved and certified forensic team will remove the potential of fines being levied by Visa for being non-compliant at the time of the cardholder data loss. Failure to be compliant can result in a very high cost per incident and allow for legal action by the owners of the data that was taken and exposed to the world.

Consequences of Non-Compliance

Companies choosing not to become compliant or allowing compliance to lapse, can face several potential consequences that may directly impact the bottom line. Potential impacts of non-compliance include:

- Fines by Visa. For each "egregious violation" companies can be fined up to $500,000.00 U.S.
- Requirement by Visa to pay for all forensics examinations to determine the "Who, What, When, How and Why" of the incident in the event of a security incident.
- Liability for the card issuer or the acquirer bank's losses as the result of a security incident.
- Dispute resolution costs.
- Restrictions imposed by Visa or other card issuers.

In most of the cases to date, the biggest monetary losses have been incurred by card issuers or the acquirer bank. The second largest cost of an incident has been the forensics examination and associated remediation to correct issues in order to prevent future incidents. So far, fines have made up the smallest of the losses experienced.

Companies may also experience negative publicity, harm to their brand image and loss of customer goodwill from the loss of cardholder information while failing to uphold the minimum standard for securing that data. These costs, while difficult to quantify, can be substantial.

Other Considerations

Protection From External Attackers is Not Enough

Putting protection in place to block external threats only covers approximately 20 percent of the losses that occur today. The other 80 percent of data losses occur from insiders that companies allowed into the systems. The failure to provide for proper care, custody and control, allowed these insiders to remove data from the systems.

The incident at the Veteran's Administration is a perfect example of the insider threat in a non-cardholder incident. The loss of 28 million veterans' records from 1975 to the present occurred due to improper controls and the lack of auditing system users.

The PCI standard looks at all the potential points of data loss, internal and external. Using a best practices approach, the PCI standard provides an auditable process to determine compliance. These standards are not so restrictive that companies are unable to accomplish business activities.

Compliance May Not Equal Security

Compliance represents a snapshot of time during an ongoing battle to maintain control of information assets. A company's ability to claim compliance indicates that they meet due diligence requirements in that instant.

Companies choosing to stay at this baseline of protection are likely to be compromised. The key to being secure is raising the degree of protection for information assets above the baseline, while reducing the cost for this protection.

Developing a security program, following a best practices framework such as ISO-17799 and integrating security into business processes can help companies not only become compliant, but more secure. Making security a part of business process can also help with ongoing compliance – reducing the time and energy it takes to achieve.

Payment Applications

Companies that develop applications for processing cardholder data may soon be required to have each version and release of the application certified. Currently, Visa is only encouraging "payment application vendors to validate the conformance of their products to Visa's Payment Application Best Practices (PABPs)[1]."

Payment application validation and certification can only be performed by a Visa trained and certified third party company that is recognized as a Qualified Payment Application Security Company (QPASC). Visa USA manages the PABP program outside of the PCI SSC.

The certification process requires substantial testing of payment applications for the vendor to render an opinion of conformance with the requirements. Visa recommends that merchants use validated payment applications (a complete list is available on the Visa Web site). Likewise, acquirers should encourage their service providers and merchants to use the PABPs to evaluate their payment applications.

More information and a list of QPASCs is available on the Visa Web site at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html.

Conclusions

Compliance with the Payment Card Industry Data Security Standard, though not legally required, is recommended for companies that store, process, or transmit cardholder data. The benefits of compliance outweigh the burden of becoming compliant.

PCI compliance is not difficult but does take time. Currently, the time from the initial pre-assessment for the gap analysis to the final submitted ROC is approximately four months. Even for companies that have been certified in the past (prior to December 15, 2005), gaining certification under the common process now is more difficult and generally requires some remediation to allow for all areas to be marked as “In Place.”

Companies that are in compliance with the ISO 17799 domains (not ISO compliant) are less likely to have an issue gaining full PCI compliance. Most companies, however, are striving for ISO 17799 compliance, so PCI certification may require some remediation to gain the necessary compliance.

Choose a vendor that is not only certified to conduct the assessments, but will also serve as a trusted security advisor. As companies grow, having a trusted advisor to assist and mentor them through the various approaches to meeting PCI certification is less costly than bidding each piece to separate vendors. Make sure to choose a vendor that is a security expert in order to gain the benefit of the vendor’s total security background and experience.

About the Author

Howard Glavin has more than 38 years of security and protection experience, including working with the United States Marine Corps, Federal Bureau of Investigation and as a Chief Information Security Officer/Director of Security for CSX Corporation. He has been a senior consultant for IBM Internet Security Systems since 2001. In addition, Glavin has developed and taught social engineering and counter-attack techniques to master’s students at Webster University. Glavin is a Certified Protection Professional (CPP) and a Certified Information Security Manager (CISM). He is also a Visa Certified Qualified Data Security Professional (QDSP) and Payment Application Security Professional (QPASP), having met the requirements to perform PCI audits and application security reviews for payment applications. Glavin holds a bachelor’s degree from Youngstown State University and a master’s degree in computer security from Ball State University.

About IBM Internet Security Systems

IBM Internet Security Systems, Inc. (ISS) is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM protection platform automatically protects against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. IBM ISS products and services are based on the proactive security intelligence of its X-Force® research and development team – a world authority in vulnerability and threat research. The IBM ISS product line is complemented by comprehensive Managed Security Services and Professional Security Services. For more information, visit www.ibm.com/services/us/iss or call 800-776-2362.

About IBM Professional Security Services

IBM Professional Security Services help reduce risk to critical business assets with comprehensive security assessment, design and deployment offerings. These proven consulting methods are based on ISO 17799 security best practices to help organizations of all sizes meet security objectives, achieve regulatory compliance, maintain business continuity and reduce overall risk. IBM Professional Security Services provide organizations with the flexibility to co-source the assessment, design, deployment, management and certification of their security posture, freeing them to focus on their core business. The IBM ISS team of expert security consultants employs proprietary toolsets, the latest threat intelligence and advanced countermeasures to help build effective security programs that protect and enhance business operations.

IBM ISS is a Qualified Security Assessor and an Approved Scanning Vendor, having met the requirements to perform PCI data security assessments globally. Security assessments are conducted by IBM ISS security experts who have in-depth experience in market and compliance requirements. ISS is also recognized as a Qualified Payment Application Security Company. ISS has met the requirements to perform PCI Payment Application Security Assessments to validate payment applications. These assessments are conducted by ISS security experts who are Qualified Payment Application Security Professionals. For more information about PCI compliance services from IBM ISS, e-mail qdsc@iss.net.

IBM Global Technology Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
06-07

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM assumes no responsibility regarding the accuracy of the information provided herein and use of such information is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

[1] Visa USA, "Open Letter to Vendors", June 2006 - http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PABP_Validation_Letter_to_Vendors.pdf