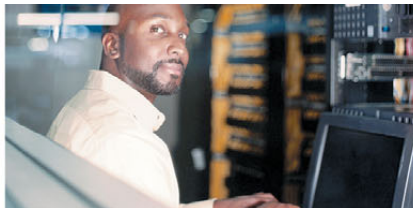




The Return on Investment of Payment Card Industry Data Security Standards (PCI DSS) Compliance





Contents

- 2 Executive summary
- 3 Rethinking PCI requirements
- 5 Mapping PCI compliance within an existing risk management strategy
- 7 New requirements: the challenge to stay compliant
- 9 The value of a third party compliance assessor
- 10 Selecting a third-party assessor
- 11 PCI Return on Investment (ROI)
- 14 Why IBM ISS for PCI?

Executive summary

In 2001 Visa developed the first credit card industry security standard called the Cardholder Information Security Program (CISP). Around that time MasterCard and other card brands also began to develop their own separate but similar security standards. After creating their own individual data security standards the major payment card brands, normally are fierce competitors, decided to work together for the overall benefit of the payment card industry. Ultimately Visa, MasterCard, American Express, Discover, and JCB became the primary founding members of the Payment Card Industry Security Standards Council (PCI SSC). They also merged some of the best concepts of their own security standards to ultimately create a single, comprehensive payment industry wide security standard—the PCI Data Security Standard (PCI DSS). Having a single cardholder data security standard helped to consolidate credit card processing security standards and associated compliance validation requirements. It also helped to reduce any merchant and service provider confusion over which standard to salute when required to process payments from many different card brands.

Compliance with PCI DSS has since become a global requirement for any business or entity that processes credit card transactions as payment for goods and services. Despite the fact that PCI compliance deadlines have come and passed, many organizations are still working very hard to achieve PCI compliance and as such are still lagging behind. Mandatory compliance with *any* industry or regulatory requirement can appear to be an overwhelming challenge. Having to comply with PCI DSS requirements might feel like yet *another* regulatory burden when so many entities already have to contend with Sarbanes Oxley, GLBA, HIPAA, etc.

Though maintaining compliance with any requirement can be a challenge, IBM believes that the PCI compliance should instead be looked upon as an opportunity for implementing qualitative improvements to data protection within an organization. By definition, it is an opportunity to help ensure the protection of sensitive customer cardholder information (CHI) as it is stored, processed, or transmitted. This is, after all, at the heart of why the original credit card security standards were initially developed and is the driving principle behind the PCI DSS.

Rethinking PCI requirements

Over the last few years there have been a number of high-profile security breaches and instances of identity theft. The financial consequences of having to investigate the cause of, and attempt to remediate the impacts of a serious data breach can be staggering. In some instances the liabilities and consequences of dealing with large-scale data theft have actually driven companies out of business. Each instance of a breach that involves the unauthorized disclosure of cardholder information has reinforced a sense of urgency to re-emphasize the protection of sensitive cardholder data. Some of the largest payment card breaches to date include T.J. Maxx involving approximately 45 million compromised customer records, and the recent Heartland Payment Systems breach has been estimated to have compromised tens of millions of credit and debit card transactions.¹

While the PCI DSS might seem like just another snarl of red tape to companies burdened with existing compliance requirements, the standard is based upon sound Information Security 'best practices'. It is comprehensive and well designed. As such, the core principles of properly securing cardholder information and protecting the systems that process it are consistent with similar requirements found in

The six areas of data protection requirements prescribed by the PCI standard address issues ranging from network protection to security governance policies.

Sarbanes Oxley, GLBA, HIPAA, etc. If a business or entity is already compliant with other standards, then much of what is required to be PCI DSS compliant may already be in place. Having to also address PCI compliance will help to further reduce unnecessary risk to existing business processes and assets. It can also produce measurable gains in business efficiency and data security.

The six primary categories of PCI

When considered together, the six areas of data protection requirements prescribed by the PCI standard help you build a comprehensive approach to securing cardholder information. They address security concerns from network protection to security governance policies.

- **Build and maintain a secure network**
 - Install and maintain a firewall configuration to protect cardholder data.
 - Do not use vendor defaults for system passwords and other security parameters.
- **Protect cardholder data**
 - Protect stored data.
 - Encrypt transmission of cardholder data across open, public networks.
- **Maintain a vulnerability management program**
 - Use and regularly update anti-virus software.
 - Develop and maintain secure systems and applications.
- **Implement strong access control measures**
 - Restrict access to cardholder data business need-to-know.
 - Assign a unique ID to each person with computer access.
 - Restrict physical access to cardholder data.
- **Regularly monitor and test networks**
 - Track and monitor all access to network resources and cardholder data.
 - Regularly test security systems and processes.
- **Maintain an information security policy**
 - Maintain a policy that addresses information security.

Compliance with the PCI Data Security Standard is a requirement for all merchants and service providers that store, process, use or transmit payment cardholder data.

Who must comply with the PCI Data Security Standard?

All merchants and service providers that store, process, use or transmit payment cardholder data must comply with the PCI DSS. The security standard is maintained by the PCI Security Standards Council, and its enforcement is maintained by the card brands as well as the financial institutions that acquire and process credit card transactions.

Mapping PCI compliance within an existing risk management strategy

The principle of risk management is consistent with the philosophical basis for the PCI DSS. In 2004, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission released an integrated framework for enterprise risk management to provide guidance and benchmarks designed to enable organizations to:

- Align their risk tolerance with strategic business goals
- Measure risk and determine how taking risks affects growth
- Create greater flexibility in risk mitigation and incident response
- Identify and correlate cross-enterprise risks
- Develop a cross-enterprise governance and risk management capability
- Respond to business opportunities with an understanding of the full range of events within the organization
- Make better capital investments by more effectively assessing risk

The core principles of the PCI security standard are consistent with critical areas of the COSO framework, as follows:

- **Event identification** recognizes the enhancements to business prospectus all while helping to ensure the protection of critical information assets including CHI.
- **Risk assessment** requires companies to realistically analyze the risks to their businesses. The PCI DSS is a risk management based approach to protect CHI and preserve card brand business integrity.
- **Risk response** helps to ensure that the most critical risk to business assets is remediated. The PCI DSS is focused on the identification and reduction of risk to CHI, but also to effective Incident Response when needed.
- **Control activities** establish clear guidelines and policies that everyone must follow, helping to boost consumer confidence and reduce the risk to their CHI.

Fortunately, the concepts of event identification, risk assessment, risk response and control activities are also relevant for compliance with a multitude of other requirements including the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and others. Adopting a risk management approach that includes the PCI DSS is entirely consistent with these other standards as well. And once again, if a business or entity is already compliant with the other standards, then much of what is required to be PCI DSS compliant may already be in place. This helps to leverage investments, and spread the costs of maintaining the Information Security framework across all relevant requirements of the various standards.

New requirements: the challenge to stay compliant

While PCI standards are concisely written and are entirely consistent with corporate governance and risk management strategy, you should be aware of a number of factors that can produce ‘speed bumps’, if you will, in the road to PCI DSS compliance. While fully supporting and mandating compliance with all of the requirements contained with the PCI DSS, each payment card company has the option, and the ability to “raise the bar” if you will. To help address specific issues or to target changes in the perceived threat profiles to CHI, the card brands have imposed additional mandates over and above those required by the PCI DSS. A good example of this is the recently announced Visa mandates for application security, which were designed to eventually eliminate the presence of “vulnerable” payment applications from the Visa’s payment processing networks. A summary of the mandates is as follows:

1. Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications. *Compliance deadline - 1/1/08*
2. VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant. *Compliance deadline - 7/1/08*
3. Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications. *Compliance deadline – 10/1/08*

4. VNPs and agents must decertify all vulnerable payment applications.

Compliance deadline -10/1/09

5. Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications. *Compliance deadline – 7/1/10*

When preparing to meet the challenge of a PCI DSS compliance assessment, you must ensure that specific security controls are in place. For example, you must be able to demonstrate that you are not storing data that the PCI DSS specifies cannot be stored. For example “sensitive authentication data” such as full-track data from the magnetic card strip, PIN information or the card validation number (CVC, CW2, CID) must never be stored following the completion of the transaction authorization process. In addition the requirement to securely delete data when no longer needed implies using a mil-spec data eradication utility such as a U.S. DoD approved data deletion utility or equivalent. In this case serious scrutiny should be given to such possible data storage repositories as database tables, system backup files, transaction logs, application logs, error logs and reports, history and trace files, etc.

PCI DSS compliance gaps are routinely identified during assessments. Among the most common errors are storage of prohibited cardholder data and lack of segregation of internal staff duties.

Avoiding common errors

It can be helpful to know that gaps with PCI DSS compliance requirements are routinely identified during assessments, and they include the following:

- Storage of prohibited cardholder data
- Use of production cardholder data in test environments
- Failure to encrypt the full Primary Account Number (PAN)
- Lack of proper network segmentation that would isolate the transaction environment
- Lack of segregation of internal staff duties
- Non-compliant software development practices

The value of a third party compliance assessor

While some companies do elect to pursue PCI compliance on their own, others find that there are certain advantages to using a third-party vendor for these activities. For some organizations, an outside vendor can provide external validation that the appropriate processes and policies are in place. This validation can be used to provide reassurance to customers, partners, shareholders and card issuers. A third-party vendor can also provide an objective analysis of your current compliance status, along with recommendations for closing any perceived compliance gaps. Because third-party PCI Qualified Security Assessors are required to provide unbiased and objective recommendations for technology and services, you are protected against a vendor simply recommending its own product solutions over others.

When compliance validation activities are executed in-house, company officials are fully liable for any omissions or errors. Using a third-party vendor does **not** shift the risk away from senior corporate management. The third party, however, can provide objective recommendations to help to reduce the possibility that compliance requirements might be overlooked. The objective third party can also help to sort through sensitive or contentious issues that might arise as differing groups within an organization try to champion conflicting agenda.

The required internal and external penetration testing of cardholder processing environments can be done in-house by properly trained company personnel. Quarterly external network vulnerability scans are also required for all merchants and service providers, and these scans must be performed by an Approved Scanning Vendor (ASV). When companies reach a certain threshold of payment card transactions (deemed a level 1 merchant or service provider), a PCI certified QSA must be engaged to assess and validate overall compliance with the PCI DSS Requirements and Security Assessment Procedures v1.2 document. The PCI Security Standards Council oversees the PCI QSA program, ensuring a defined level of professional and technical competency. All QSA's must undergo annual re-training and re-certification by written examination.

Selecting a third-party assessor

Asking a third-party assessor to sift through your critical data review the configurations of production payment processing systems can be an uncomfortable proposition for some. It is important to choose a trusted, experienced, certified provider that not only fully understands the PCI DSS, but also fully comprehends its impacts

to your business and associated business processes. They should have the ability to handle all phases of PCI compliance assessment and validation; from pre-assessment through Report of Compliance (ROC), and Attestation of Compliance (AoC) submission. Your QSA should also be willing to offer you multiple alternative solutions to resolve potential compliance gaps. It would also be extremely valuable if the assessor's core competencies extend well beyond PCI compliance services, and also help to address your organization's overall security posture.

As you proceed through the selection process, it might be helpful to ask these questions:

- What am I getting for my investment?
- Do I receive simply a final report, or do I benefit from the assessor's overall security expertise and competencies?
- How flexible can the assessor be to accommodate "compensating controls"?
- Is my QSA currently certified?
- Has the QSA ever been placed on remediation or probation by the PCI SSC?
- Has this vendor fully explained the timeline involved for the PCI compliance process?
- Can and will the QSA assist in negotiations with acquiring banks and the card brands.

PCI Return on Investment (ROI)


While some have tried to assert that PCI compliance can be seen as a potential contributor to a company's 'bottom line', the real truth is that it can often require a significant enhancement to existing resources. Given this fact, how then can PCI compliance help to enhance an organization's profitability?

For those entities that process credit card transactions, PCI compliance is not an option. As such there may indeed be a need to “invest” in the additional personnel and resources required to adequately protect customer credit card information and privacy. Since managing risk is a part of doing business, critical information assets must be protected from risk or undue harm just like any other corporate asset. Reducing potential risk to critical assets helps to ensure and even enhance their value and that translates into a value proposition for the business. As your PCI compliance effort begins to spread throughout the organization, personnel who might have previously given little thought to company privacy and security policies may become aware of their own personal contributions to this cause. After all most personnel have and use credit cards. Some may have even been notified by their banking or other financial institution that their personal information had possibly been compromised.

PCI compliance can touch many throughout an enterprise; managers, technical support personnel, sales and marketing staff, business account managers, senior executives, HR, customers, etc. As they become aware of their possible role in helping to protect CHI and associated systems, the protections and enhancements brought about by pursuing PCI compliance will proliferate with them. When customers, business partners and service providers realize this there will be a measurable and significant enhancement to the quality of business relationships. In addition reducing risk to critical information assets can help to reduce business overhead, maintenance, and insurance costs. Reducing the risk of a possible breach of critical corporate information assets provides measurable enhancements to corporate brand recognition and customer confidence. Your customers know you care about their business, and will be a proper custodian of that which they deem most sensitive; their personal cardholder information.

There is an old saying that simply states "...a rising tide floats all boats". Implementing a cardholder information security program based upon PCI DSS within an organization will help to reduce the risk to all business assets across the enterprise. It is also an investment that provides many returns over time.

Proprietary Tools and Technologies from IBM include:



IBM helps simplify compliance with a deep portfolio of proprietary tools and technologies.

- IBM Tivoli® Security Information and Event Manager helps clients monitor the activity of privileged users. The product collects, centralizes and archives relevant security log data from heterogeneous sources, filtering collected information against requirements and corporate security policies, and provides consolidated viewing and reporting through a central, compliance-oriented dashboard.
- IBM Tivoli zSecure helps ensure the security of mainframe systems by automating administration and auditing. Tivoli zSecure Audit, a component of the Tivoli zSecure suite, offers the capability to fingerprint sequential log data residing on both tape and direct access storage device (DASD) media to check the integrity of System Management Facility (SMF) logs.
- Tivoli Key Lifecycle Manager – provides centralized and automated encryption key management. It enables an organization to fully document and implement all key management processes and procedures for keys used for encryption of cardholder data.
- IBM Rational® AppScan® helps manage Web application security throughout the software lifecycle: audits Web applications, tests for security and compliance issues and provides actionable reports with fix recommendations.
- IBM Internet Security Systems™ (ISS) solutions: provide a protection platform that is designed to automatically guard against both established and unknown Internet-based threats and is driven by the advanced analytics developed by the IBM Internet Security Systems X-Force® research and development team.

Additional IBM hardware, software and services (including IBM Tivoli software, IBM System z® encryption solutions and the IBM Resource Access Control Facility [RACF®] program): help optimize security, compliance, and the alignment of business and IT.

Why IBM ISS for PCI?

The IBM ISS Global PCI Security Practice is one of four entities recognized as a Global PCI solutions provider. IBM ISS is also a Qualified Security Company (QSC), and can provide Qualified Security Assessors for PCI DSS and PCI PA-DSS compliance assessments. IBM ISS is also a PCI SSC recognized Approved Scanning Vendor (ASV). IBM ISS provides incident response services to help investigate possible PCI breaches to assist in determining whether a breach has occurred and to guide with remediation next steps.

IBM maintains a staff of highly-skilled, certified security professionals who have industry-specific expertise and use consulting methods based on Information Security best practices. These abilities help us go beyond simply assessing your PCI compliance status to providing detailed recommendations for creating a comprehensive security strategy.

What's more, IBM's proprietary technologies and tools help you build a strategy to maintain compliance. We take pride in being a trustworthy resource with a strong track record of customer satisfaction in confidentially handling sensitive data.

For more information

To learn more about PCI compliance and how IBM can help, please contact your IBM marketing representative or IBM Business Partner, or visit the following Web site: ibm.com/services/security





© Copyright IBM Corporation 2009

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

Produced in the United States of America
July 2009
All Rights Reserved

IBM, the IBM logo, ibm.com, Internet Security Systems, X-Force, Tivoli, System z, RACF, Rational and AppScan are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

Other product, company or service names may be trademarks or service marks of others.

¹ http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html



Recyclable, please recycle