



# CHAIN STORE AGE<sup>®</sup>

THE NEWSMAGAZINE FOR RETAIL EXECUTIVES

July 19, 2007

<http://www.chainstoreage.com/csa/guestcomm/>

## **Policy: Where It All Begins for PCI Compliance**

By Ed Adams and Michael Gavin

PCI compliance can be intimidating because it is a highly prescriptive, broad-reaching set of requirements, potentially including all of your information systems in its scope. This article provides organizations with practical advice and tips from Security Innovation, a Qualified Security Assessor Company (QSAC).

### ***Do I need to comply?***

Though the PCI Security Standards Council defines and builds the global Payment Card Industry Data Security Standard (PCI DSS), each card brand, e.g., Visa, MasterCard, Discover, American Express and JCB, enforces it via its compliance program and dictates the validation steps and documentation required to show compliance. Even though you obtain “PCI compliance” by passing a PCI Audit and filing the required paperwork, each brand maintains its own tracking, penalties, fees, rewards and acceptance process for compliance filings.

Generally, if you store, process, or transmit cardholder data—e.g., a primary account number—from any brand, you must comply with PCI DSS and the brand’s compliance program. This includes merchants, banks and service providers from all industries, e.g., bricks-and-mortar retailers with a point-of-sale terminal, MOTO merchants (mail order, telephone order), payment gateways, transaction processors, and credit-reporting services. Brand-specific documentation requirements and compliance levels may be found on each brand’s Web site.

### ***The 12 Requirements***

The PCI DSS requirements apply to all system components, which are defined “as any network component, server, or application that is included in or connected to the cardholder data environment.”

The DSS specifies which cardholder data must be protected if stored, and which cardholder data is not allowed to be stored at all once the card has been authorized: the Card Validation Value or Code, the PIN or PIN Block, and the full magnetic stripe. Storage of the primary account number (PAN), cardholder name, service code and expiration date is allowed if that data is sufficiently protected as specified in the DSS. However, you should carefully consider whether you actually need to store cardholder data at all. You shouldn’t store cardholder data you don’t absolutely need to conduct

business and to process transactions; further, you should store cardholder data only for as long as you need it.

The 12 PCI DSS requirements are grouped into six categories created by the PCI Security Standards Council:

1. Build and Maintain a Secure Network;
2. Protect Cardholder Data;
3. Vulnerability Management Program;
4. Implement Strong Access Control Measures;
5. Monitor and Test Networks, and
6. Maintain an Information Security Policy.

### ***Policy—Where Compliance Begins***

There are three major areas which, if managed correctly, can save you much time and money during your PCI audit and simplify continuing compliance:

- Policy
- Network Segmentation
- Applications, Vulnerability Management, and Testing

When put into practice effectively, these focal areas can help you define, implement, enforce, and maintain a strong information security program with the side effect of also being PCI-compliant in the process.

Policy is the foundation upon which a stable, maintainable information security program is built. Proactive and progressive organizations see the PCI-compliance requirements as a catalyst for adopting a philosophy where security is the objective and PCI compliance is achieved in the process.

For policies to be useful you must tailor them to your business; they must address your specific business needs, processes, assets and environment. The primary objective of creating security policy is to ensure that your business-protection needs are being met. When creating the policy to satisfy that objective, you must structure your policies so that they can be implemented and enforced.

Taking the relevant steps from a risk-management process and applying them to PCI compliance yields the following basic steps you should take:

- Identify your information and data assets;
- Define your risk tolerance and acceptable treatments, e.g., avoidance, reduction, retention, and transfer;
- Identify access controls and handling practices for your data, i.e., who has access and what can they do?
- Decide how you want to protect your assets and to what extent. This should include an incident response plan and the definition of consequences so when implemented you can also enforce it;
- Communicate and share your policy information, i.e., educate your organization on

your information security policy;

- Iterate the policy as needed (ideally based on feedback from step 5);
- Implement, monitor and enforce;
- Compare your policy to PCI requirement 12.

The result of the process above will be the construction of a policy baseline—a foundation that sets off boundaries for acceptable data handling across your organization. The results are: better business relationship and communication between groups; the ability to self-analyze your information security state; security awareness throughout your organization; and a consistency with which to measure and test your information security practices.

Finally, note that the 12 PCI DSS requirements correspond to 233 auditable statements and testing-procedure validations. Requirement 12, “Maintain a policy that addresses information security” comprises 39 of these statements, while many of the others will also directly correspond to elements of your information security policy.