ecora

WHITEPAPER

Using Automated, Detailed Regulatory Compliance and IT Best Practices Reporting to Achieve and Maintain Compliance with the Payment Card Industry (PCI) Data Security Standard

Alex Bakman
Chairman and Chief Technology Officer
Ecora Software

Introduction

Until recently, ensuring compliance was most often viewed as an event rather than as a critical, ongoing business process. Taking a tactical approach, an organization would learn of an upcoming audit and then begin to prepare documentation and gather information in what was often a time-consuming and cumbersome manual process.

Today, however, with the growing pressure of government compliance requirements and industry regulations, ensuring continuous compliance need to become integrated into the way an organization does business. And, as is the case with any integrated business process, the ability to simplify and automate the process has had to become essential.

One new standard that is changing the way many organizations operate is the Payment Card Industry (PCI) Data Security Standard.

When customers use their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is secure. To that end, in June 2001, Visa developed the Cardholder Information Security Program (CISP), a mandated security program for large Internet merchants. In 2004, all major bankcards—Visa, MasterCard, Discover, and American Express—agreed to adopt a single, unified security program as the standard for data security. The new standard, called the Payment Card Industry Data Security Standard or PCI, is intended to protect cardholder data—wherever it resides or is transmitted—and requires that merchants and service providers that store, process, or transmit cardholder data meet specific security requirements. Ultimately, PCI offers a systematic approach to safeguarding sensitive data for all card brands.

Why Is PCI Compliance Important?

Ensuring compliance with the PCI standard is important for a number of reasons, but perhaps the most significant reason is to **protect brand reputation**. The public scrutiny that accompanies any breach in security can be very damaging to an organization's image. Any organization doing business in California, for example, is required to disclose any security breach publicly under state regulation CA-1386, and there is no faster way to lose customer confidence than to be forced to report publicly that credit card numbers have been stolen. In fact, a recent study by the Polemon Institute reports that data breach disclosures, in time, will result in the loss of as many as 20 percent of existing customers.

The second reason for ensuring compliance with the PCI standard is to **avoid fines and additional regulatory scrutiny**. Failure to comply with the PCI Data Security Standard can result in fines that range from $200,000 to $500,000 per security breach, as well as additional government-levied fines that can range from $5 million to $20 million. In addition, once an organization has failed a PCI audit, it is given an elevated risk status and becomes subject to more extensive PCI audits. The ultimate penalty can be a suspension of status and the loss of the ability to accept and process credit cards.

Some organizations have even been forced out of business by a violation of the PCI Data Security Standard.

Who Must Be In Compliance?

At the most fundamental level, any company that comes into contact with credit card information must be in compliance with the PCI Data Security Standard.

There are varying levels of compliance proof or validation, however, with specific requirements for merchants and specific requirements for service providers, as well as various levels based on the number of transactions processed annually. A merchant that processes more than six million Visa transactions each year is assigned to "level 1," as is an organization that has experienced a security breach, for example. Those at level 1 are subject to significantly higher levels of scrutiny than merchants at level 2, 3, or 4.

For service providers, there are three levels of compliance. Level 1 encompasses members and non-members of all payment gateways. Level 2 is made up of service providers who process more that one million transactions annually, and level 3 includes any service providers who are not in level 1 and who do less than one million transactions in any given year.

Audits for PCI compliance vary depending on a merchant's or service provider's level.

- **Merchants at levels 1 – 3 and all service providers must complete a quarterly network scan** through a certified PCI vendor. Auditors then present the results of the scan to the compliance agency.
- **Merchants at level 1 and service providers at levels 1 and 2 must also complete an annual on-site security audit**. Even compared to Sarbanes Oxley, Gramm-Leach-Bliley or HIPAA audits, the PCI on-site audit is very thorough and tightly managed by the governing body. Ideally, preparation for this audit should be automated.

		COMPLIANCE ACTIONS	VALIDATION ACTIONS		
Group	Level	Comply with PCI Data Security Standards	On-Site Security Audit	Self-Assessment Questionnaire	Network Scan
Merchant	1	Required	Required Annually		Required Quarterly
	2 & 3	Required		Required Annually	Required Quarterly
	4	Required		Recommended Annually	Recommended Annually
Service Provider	1	Required	Required Annually		Required Quarterly
	2	Required	Required Annually		Required Quarterly
	3	Required		Required Annually	Required Quarterly

- **Merchants at level 2 and 3 and service providers at level 3 must undergo an annual PCI data security assessment**, which can be performed by a certified on-site PCI auditor or using an internal audit function.
- The requirements are less stringent for **merchants at level 4**, which present a completed questionnaire as proof of compliance, but ensuring compliance with the PCI standard is still essential.

Meeting the PCI Data Security Standard Requirements

The Payment Card Industry Data Security Standard establishes twelve requirements that companies must follow to ensure the security of credit card data. These requirements span every aspect of an organization's operation—from business processes to the configuration of the IT infrastructure—and fall into six major control objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data. One of the most critical elements of the PCI standard is the concept of separating the network and the systems involved with processing credit card data—including firewalls, routers, and switches, operating systems, database management systems, and applications—from the rest of an organization's IT infrastructure components.

Under this requirement, it is essential that firewall configuration standards are set and that credit data is protected. One best practice is to use VLANs to physically isolate the traffic involved in credit card processing, which protects a customer's data and ensures that only this part of the infrastructure is subject to PCI audit.

Organizations will also need to demonstrate a solid change management process, so that proposed changes to configurations, firewalls, and routers are thoroughly reviewed, an impact analysis is performed, and the impact of the changes is understood.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. This requirement may seem obvious, but it remains essential to evaluate all PCI-related IT components and generate lists of the default passwords, user IDs, and passwords. In the Windows environment, for example, service accounts created under a system administrator's personal credentials are a good target for review. Organizations must take a holistic view of each layer and of every component that is involved in PCI activity, and make sure that all the default system passwords have been disabled and the service accounts have either been disabled or that there is a legitimate reason for them to exist in the first place.

Protect Cardholder Data

Requirement 3: Protect stored data. This requirement begins with the encryption of any information that concerns credit card data. It is a very challenging requirement for many organizations to meet, in part because of performance expectations and the complexities created by system integration. Organizations have to maintain a good track record of cryptographic keys and ensure there is a policy in place so that only those with a "need to know" have access. Managing this requirement extends through the entire IT system, from the point-of-sale or website to the data center.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks. This requirement ensures that any traffic going over the public Internet, whether inbound to or outbound from an organization's website, is encrypted. Organizations may meet this requirement using a number of technologies, including Secure Socket Layer (SSL), IPSec, WPA, and WPA2.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software. Anti-virus software provides the first line of defense; organizations need to ensure, and demonstrate, that the latest signature file is distributed regularly, to both client-side and server-side systems.

Requirement 6: Develop and maintain secure systems and applications. Under this requirement, an organization ensures that the entire infrastructure involved in credit card processing is updated as soon as security patches are provided. PCI auditors look for specific evidence that this practice is taking place in the environment.

Another part of the requirement mandates adequate testing before a patch is applied to production systems and that a solid change control process is in place for all systems and self-reconfigurations. PCI auditors are concerned with how frequently an organization upgrades applications, the quality processes involved, whether there is a traceability index, and whether they can pinpoint specifically what changes have been made to each application.

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know. To meet this requirement, organizations must document each specific function in processing a credit card transaction and demonstrate that each staff member performs that function only. They must also show who has access to which systems and data. This delineation of functions helps ensure that no one in the organization has access to the entire procedure for processing credit card data.

Requirement 8: Assign a unique ID to each person with computer access. Organizations should have a written policy in place, signed by each employee, that states that all IDs and credentials are to be used solely by the individual to whom they are assigned. Organizations should also ensure that they have a policy for password aging and that password aging can be verified and validated. If, for example, an organization has a policy that passwords should be changed every thirty days, they should be able to prove that passwords are actually changed within that timeframe.

In addition, organizations should be able to demonstrate that there is an automatic provisioning process in place for new hires and for employees who transition to other positions within the organization, as well as to ensure that credentials are immediately suspended for an employee who leaves the organization.

Requirement 9: Restrict physical access to cardholder data. To meet this requirement, organizations need to monitor access in sensitive areas, deploy procedures to track those who enter or leave the environment, and ensure that audit trails are stored in a safe location, in an encrypted format, and with good physical security.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data. Organizations must track and monitor all access to network resources and cardholder data—including during day-to-day, real-time, and dynamic events. To do so, organizations must have a clear policy about the kinds of data being logged and ensure the integrity of the data being logged. Importantly, only those who "need-to-know" should have access to credit card-related data, and organizations should have an audit trail in place.

Requirement 11: Regularly test security systems and processes. To meet this requirement, organizations will need to demonstrate that they undertake regular testing to ensure that all other requirements are met. The quarterly vulnerability scan, which focuses on penetration testing from the outside, comes into play here, as well as capabilities in place for integrity checking within the organization.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security. A recent article in *ComputerWorld* indicated that only thirty percent of companies have a written security policy in place, yet a written security policy is the basis for an organization's solid security practice. It is also essential to fulfilling the requirements of the PCI audit.

How Ecora Software Can Help

Ecora Software can help organizations demonstrate compliance with nine of the twelve basic PCI requirements, enabling them to pass key PCI audits efficiently, painlessly, and successfully.

Ecora's automated software solutions discover an organization's critical systems and collect configuration data—including security-related data such as credentials, permissions, access controls, and more in a centralized Configuration Management Database (CMDB). Importantly, the information stored in the CMDB enables organizations to generate reports to assess controls and identify who has access to which systems and data, validating that the current environment matches mandated standards. These reports are a critical part of passing PCI audits and are designed to be easily understood by auditors. Report packs that map specifically to individual PCI requirements are pre-installed. Additional report packs are included for Sarbanes Oxley,Gramm-Leach-Bliley, HIPAA, and FISMA requirements.These reports are also beneficial for validating compliance with other internal IT initiatives.

The way to meet IT audit and compliance requirements without a substantial investment of time and resources is through automation, but only if an organization has the ability to identify and report on the entire infrastructure. Ecora's software solutions cover all critical infrastructure components, from operating systems, to network devices and firewalls, to mail servers, to application enablers, to directory services—automatically collecting hundreds of thousands of critical configuration settings needed to recover, secure, report on, and track infrastructure changes.

Nearly every aspect of PCI begins with a baseline, and Ecora software enables an organization to take a baseline of the existing environment so that changes can be tracked against the baseline. Organizations capture granular information about baseline variance and generate specific reports to demonstrate what is taking place in the environment. The consolidated change log, for example, meets one of the key requirements of the PCI audit.

To be successful, an organization needs to demonstrate that they have control of change in their environment. Consider this: an environment where change takes place without control or review is automatically a red flag for auditors.

At the same time, however, any steps put in place to ensure a successful PCI audit can have far-reaching implications for other parts of the environment. In fact, the ability to control change will not only help ensure ongoing compliance, but also improve underlying problem management and change management processes.

Find Out More

To learn more about about how Ecora can help you achieve and maintain PCI compliance, call **877-923-2672**, email **sales@ecora.com**, or visit us on the web at **www.ecora.com.**

About Ecora

Proven in nearly 4,000 worldwide customer sites, Ecora's leading enterprise-wide audit and compliance management solutions are designed to reduce the time and costs associated with managing IT configuration controls, for enhanced infrastructure security. Ecora provides automated, centralized solutions to collect, analyze, and report on the most in-depth, multi-platform configuration information across enterprise operating systems, applications, databases, and networking devices. Ecora works to optimize IT environments and delivers an immediate return on investment. For more information about Ecora, visit **www.ecora.com**.

ecora