

The PCI Dilemma



Today, all service providers and retailers that process, store or transmit cardholder data have a legislated responsibility to protect that data. As such, they must comply with a diverse range of regulations and industry mandates. One of the most important for the service provider and retailer is the Payment Card Industry Data Security Standard (PCI DSS), which sets forth 12 requirements for IT controls to ensure data security and protection. However, retailers both large and small face tremendous challenges in implementing policies and controls that enable PCI compliance, and the task of implementing best practices can be overwhelming.

Fortunately, Tecforte's LogRadar is simplifying and accelerating the process of PCI compliance by enabling retailers and service providers to use log data generated from servers, network devices, appliances and applications to monitor, enforce and report on security policies. Logs that are well managed, offers a wealth of insightful information for improving processes across the enterprise, helping to mitigate security and performance risks and remediate incidents quickly should they occur. LOGRADAR is designed as a best practice and compliance enabler. For instance, requirement 10 and others of the PCI standard specifically mandate the use of logs for achieving compliance.

This white paper discusses the challenges organizations face in complying with PCI, and how effective LOGRADAR can simplify the compliance process while helping to improve enterprise security. It also provides suggestions for how to best prepare for a PCI audit and improve your chances of achieving on-going compliance.

PCI DSS Payment Card Industry Data Security Standard - technical and operational requirements that were created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats.

More than meets the eye

People with malicious intent will always dedicate time and resources to figure out how to infiltrate security barriers. First of all, the deployment of security policies across a large retail chain takes months, even years. By the time it's complete, the technology could be obsolete and easy for a hacker to get around. Also, there are many technology projects that are implemented without security in mind—retailers on the cutting edge using wireless technologies, for example, are not always taking the time necessary to ensure the solutions are secured.

Despite the growing threat of hackers breaking into retail networks and stealing credit card data, most retailers have not yet implemented the necessary security policies and practices, and are failing PCI audits. Recent statistics gathered by Visa U.S.A. show that only 65% of the largest retailers were PCI compliant as of August, 2007 (see Chart).



VISA U.S.A Cardholder Information Security Program (CISP) PCI DSS Compliance Validation Update as of 8/31/07*

CISP Validation Category (Visa transaction / year)	Population	Estimated % of Visa Transactions	PCI DSS Compliance Validated***	Initial Validation Submitted / Remediating	Initial Validation in Process	Pending Commitment
Level 1 Merchants** (>6M)	327	50%	44%	54%	2%	0%
Level 2 Merchants (1 - 6M)	729	13%	38%	44%	18%	0%
Level 3 Merchants (e-commerce only 20,000 - 1M)	2494	<5%	54%	20%	24%	2%

* Validation statistic based on merchant compliance reporting provided by acquirers.

** Includes Level 1 and Level 2 merchants identified from 2004 through 2006, which are required to validate by 9/30/07 and 12/31/07 respectively. Level 1 and Level 2 merchants identified as such in 2007 must validate compliance by 9/30/08 and 12/31/08 respectively.

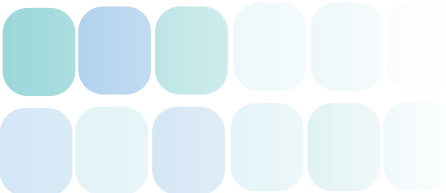
*** Noteworthy, 98% of Level 1 and Level 2 merchants confirmed that they do not store prohibited data. Acquirers of Level 1 and Level 2 merchants that continue to store prohibited data are subject to monthly fines.

Compliance is not an easy task. The strict requirements of PCI pose a huge amount of challenges to the retailer. One of the most pressing concerns is how to pass the PCI audit without taxing budgets and corporate resources. PCI offers a single set of guidelines to be applied to all sorts of retailers—both large and small. Therefore it must be very broad. PCI must cover the issues faced by an incredibly diverse group of companies—from the department store chain down to the clothing’s boutique, and companies often find themselves implementing measures that they don’t really need for their specific business simply to comply. Furthermore, this broad approach creates confusion: IT professionals and company executives must interpret the mandates in terms of their businesses, and it’s not always clear how they apply.

Another issue is the value of implementing security measures. By nature, CFOs and retail CIOs are often not on agreeing terms: security in retail has a challenging ROI argument. In other words, it’s hard to justify spending capital on security upgrades. Zero liability plans offered by credit card companies make customers comfortable with handing over their account numbers. They’re not afraid of their data getting into the wrong hands. Plus, large security breaches such as the highly publicized breach at TJX are relatively uncommon. Even following a large breach, most customers don’t associate the problem with the store they shopped in, because they don’t make the connection between the parent company, for example TJX, and the retail chain, Giant.

Some retailers have opted to self-audit, which creates further problems and inconsistencies. Those tasked with the audit might not have the required knowledge or experience to ensure compliance or identify areas of non-compliance. As a result, a company might think it’s compliant but not be, and continue to leave itself vulnerable to security breaches. Also, according to recent studies, most retailers surveyed use compensating controls—controls that have the same approximate effect as those outlined in the PCI standard, but don’t exactly comply with the standard.

For those who don’t self-audit, another problem arises. Many companies feel that there is a conflict of interest among third-party auditors hired to perform the PCI audit. Auditors who are checking security readiness and making recommendations for technology upgrades and retrofitting are often in the business of selling the products and services they recommend. Company executives wonder if the auditor is recommending the upgrade because it is the best thing, or simply to increase sales.



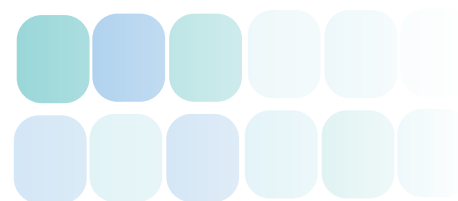
Why LOGRADAR for compliance?

An important step in establishing a compliance strategy is to implement a strong Log Management solution, one that comes with intelligence, which can help to simplify and accelerate compliance while addressing many of the challenges retailers face. Log collection and reporting—a key component of LOGRADAR—is the only efficient way to create audit trails of network and system activity—now essential for compliance and risk mitigation in complex environments. The LOGRADAR solution, which begins with log collection, gather logs from critical systems, such as applications, databases and servers, and store them securely and unaltered in a centralized location for easy reporting, searching and storing. By regularly reviewing logs, you can see failed logins, denied access attempts, unusual usage patterns, and get a fingerprint of network activity.

Alerting is another important capability that LOGRADAR provides. On-going monitoring implies real-time analysis and response in case action is needed. The ability to send alerts to key personnel when an event occurs is critical. Alerting allows us to monitor the logs and notify an operator if immediate action is needed.

LOGRADAR allows you to create reports on collected log data, which is very important for compliance efforts. Both real-time reports and historical reports are important, so both short and long-term storage capabilities are essential. An efficient log management solution must allow organizations to store logs in their raw, unaltered form to ensure data integrity and forensic utility, and in a central repository for fast access. The ability to quickly search thorough large amounts of log data for investigative purposes in invaluable for incident response.

Finally, LOGRADAR must allow for simplified yet secure log sharing. Typically, compliance is a multi-team effort that involves personnel from security to IT to management. Once the logs are collected and stored, fine-grained access control is essential to ensure that data is shared only with authorized stakeholders.





Validating controls and policies with LOGRADAR

LOGRADAR can be used to validate PCI controls and processes. For example, if you set a policy that VPNs can only be used at certain times, and someone accesses the network over a VPN connection outside of those times, the logs provide direct evidence of someone breaking the policy. Logs also provide proof of change management procedures, such as router re-configurations, firewall rule additions and the like.

Finally, logs demonstrate that IT staff is actually performing the compliance activities they claim to be performing—another PCI requirement. For example, when an employee is terminated, most companies require IT to terminate network access immediately, and in fact PCI requirement 8.5.4 also requires this. Normally, to ensure the access was blocked, IT staff would have to get a list of terminated employees, then look in the user access files to validate the access was terminated. However the act of terminating a user will generate a log message, which the LOGRADAR solution will collect and store. This message now serves as evidence of the termination procedure.

Table 1 maps PCI requirement to the log management function that addresses it.

Security		
	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
	Requirement 11	Regularly test security systems and processes
Change Management		
	Requirement 6	Develop and maintain secure systems and applications
Identity and Access		
	Requirement 7	Restrict access to data by business need-to-know
	Requirement 8	Assign a unique ID to each person with computer access
Monitoring and Reporting		
	Requirement 10	Track and monitor all access to network resources and cardholder data

Ready, set, audit!

It's likely that you won't pass your PCI audit on your first try. More typically, auditors make initial suggestions for improving processes to come closer to passing the audit. But your chances of satisfying requirements are better if you prepare ahead of time. Here are some important pre-audit activities that can help you get ready:

- 1) **Implement an LOGRADAR solution now**—LOGRADAR enables sustainable compliance and a significant reduction in risk by delivering real-time, automated alerting and reporting on policies and controls that are mandated by the PCI standard. Companies with sufficient log management in place can reduce the duration of the audit and improve the accuracy of data presented to auditors. LOGRADAR enables an ease of attestation, because reports can be generated quickly, even on substantial amounts of data. Solutions that support automated report generation can shave hours, days or even weeks off the auditing process, saving you time, money and resources. Also, look for solutions that offer log process auditing to provide evidence—automatically—that processes mandated by PCI are being implemented on an ongoing basis.
- 2) **Review the audit checklist**—IT professionals can obtain a PCI audit checklist at www.pcisecuritystandards.org ahead of time to help them identify areas of non-compliance that are obvious. These are the same audit procedures that will be used by the onsite auditors, and knowing what's on the auditor's checklist before the audit begins can eliminate many of the potential problems and pitfalls and help the process go more smoothly. Remember, although the initial goal of PCI compliance is often to pass the first audit, the long-term goal is security. For that reason, it's important to approach the audit checklist from a security standpoint—you want to protect the cardholder data.
- 3) **Determine the scope of compliance and the audit**—What are the guidelines for defining what systems are subject to PCI? Generally, only a subset of your IT systems and applications will be subject to the audit. Identify what's in scope early.
- 4) **Get to know your auditor**—Before the audit begins, meet with your auditor to discuss what systems, tools, documentation and resources they'll need to access. Obtain user credentials and authorizations ahead of time to speed up the process. Remember, the auditor is not the enemy. Don't be offended by his critiques and suggestions; he's trying to help you. Leverage his knowledge to improve your processes and achieve on-going PCI compliance.
- 5) **Embrace the audit findings plan for remediation**—Ideally, you should establish some guidelines for reviewing, prioritizing and managing remediation following the audit. For example, determine ahead of time who will be involved in the remediation effort. Establishing the remediation process up front will increase your efficiency.

