



Triumphant™

Triumphant PCI DSS Compliance Overview

White Paper
Maintaining Continuous Compliance with
PCI DSS Requirements

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) has in recent years emerged as a de-facto best practices security approach in the payment card industry. A descendent of the established ISO-17799 security standard, PCI's predecessor was developed originally by VISA as part of its Cardholder Information Security Program (CISP) in 1999.

Becoming PCI compliant, at least initially, is a challenging yet surmountable process. Re-asserting compliance in following audits is significantly more difficult, and maintaining compliance between audits is an even greater challenge, though provides significant value to organizations. Breaches inevitably lead to association or court appointed audits, and an inability to demonstrate that the breach was not a result of a failing control will likely lead to undesired conclusions. This explains the growing trend among leading IT teams to seek and implement compliance tools that are designed to support continued compliance.

Initially provided as a strong recommendation to retailers and payment processors, the past few years have seen increased compliance requirements, enforcement, and ultimately a revised technical standard known today as PCI. The standard itself is no longer specific to VISA, having been adopted by six leading card brands (VISA, Mastercard, AMEX, Discover, JCB and Diner's) as the technical foundation for their own security compliance program. It is managed by a dedicated group, the PCI Standards Council, which takes care to evolve the standard and supporting documentation over time, including the auditor requirements.

PCI has rapidly emerged as more than simply a contractual commitment between merchants and credit card associations. With strong enforcement in the form of financial penalties, reimbursement costs, higher transaction fees, and lost reputation, not to mention the potential

loss of ability to process card transactions, PCI has quickly become a de-facto enterprise security framework in the retail industry. While not a framework in the typical sense, including mainly the data protection elements of ISO17799, enforcement has increased PCI's stature and adoption rates. Furthermore, it appears that PCI is spreading into additional verticals, such as insurance and healthcare, where premiums are often paid by consumers using credit cards. Even the internet communications industry is impacted, with Internet and Alternate Service Providers (ISPs and ASPs) falling into scope due to handling of cardholder data on their networks.

Many of these organizations are finding that compliance is challenging to attain, but even more so to maintain, due to the nature of related audit procedures.

PCI TENETS

Based largely on ISO17799 provisions, PCI details a comprehensive approach to protecting data classified as sensitive. While PCI requires the development of a data classification policy, it assumes that certain types of data have already been classified as sensitive, and lists all the measures that must be in place in order to protect them.

This class of data, called "Cardholder Data", is defined as certain transaction records that appear together with a specific key. The key is called "Primary Account Number" (PAN), and generally refers to credit card account numbers, although it also includes other data such as checking or debit account numbers. The existence of a PAN in a record, results in the classification of other portions of the record as Cardholder Data, specifically the account holder's full name, service code and expiration date of the account in question. Furthermore, PCI defines Sensitive Authentication Data—data that includes magnetic stripe or CVV data and PIN blocks—as entirely prohibited from storage, regardless of protection mechanisms.

The PCI standard defines 6 major criteria, further divided into 12 major requirements, each handling an aspect of data protection, as follows:

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

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

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

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

HOW COMPLIANCE WORKS

The word “compliance” has been misused in a number of different contexts when it comes to PCI, creating confusion. It is important to understand the various steps of the compliance process in order to properly handle compliance in any impacted entity.

Basically, the process of compliance has three distinct portions: adherence, validation, and registration.

Adherence is the process of identifying gaps and establishing controls to address those gaps as closely as possible to the standard’s requirements. This part is also commonly referred to as the “dry audit” or “pre audit” and “fix-it” stages.

Validation is the process of formally assessing an entity’s adherence to the standard. This is commonly referred to as the “compliance audit”.

Registration is the process of submitting paperwork to the proper entities—normally acquiring banks or the associations themselves, depending on each association’s rules—indicating a complying entity’s adherence to the standard. This paperwork normally includes the results of the validation stage, or audit, and can take various forms; for example, a Report On Compliance (ROC) or Self-Assessment Questionnaire (SAQ).

All of these steps are collectively and individually called “PCI compliance”. Note that “compliance,” technically, should only refer to the last step in the process—registration—because only then is compliance established with each association’s compliance program rules. And it is not a uniform process, either; each credit card association has its own rules about how to report on an entity’s compliance, and different reporting requirements based on different sets of criteria (usually around the annual volume of transactions). For example, VISA defines a level-1 merchant as one that has over 6 million annual VISA card transactions across all payment channels, and requires a ROC from such a merchant submitted through a VISA acquiring bank. AMEX, on the other hand, defines a level-1 merchant as one having over 2.5 million AMEX transactions annually, and requires submission of quarterly vulnerability scans through a Trustkeeper portal.

THE ROLE OF EVIDENCE

Based on the discussion above it follows that there is a difference between standard compliance and associa-

tions' program compliance. The former requires full adherence to the entire PCI standard. The latter requires satisfying each compliance program's reporting requirements, which could be reduced in scope.

Whatever the case may be, **evidence of compliance with—or adherence to—the standard** is the determining factor in a successful audit. Such evidence takes many forms, such as screen captures, audit trails, written policies, incident reports, etc. The more comprehensive the evidence, the easier it is to satisfy the auditing criteria and consequently, the auditor.

Of course, simply providing a mountain of evidence to an auditor is somewhat self-defeating. It is preferable if such evidence can be targeted at the audited elements, allowing the auditor to more effectively audit compliance with each element. In other words, targeted audit reports, specifically addressing distinct compliance elements, provide the best form of evidence for audit. Assuming they are automatically generated and can be shown to be fully reliable, they can be considered "audit-grade."

One factor to keep in mind is that PCI compliance is generally a "binary" determination. There is no "gray area," and one cannot be considered "90% compliant." Rather, compliance is "black or white"—determined simply on the basis of whether an organization meets the entire standard, with all requirements, or not. The available evidence must therefore support every single one of the 200+ sub-requirements that are part of the PCI standard. Exceptions are made for those requirements that are not relevant to the organization, and controls that cannot be met directly can be met instead through the use of compensating controls.

COMPENSATING CONTROLS

Compensating controls are controls that are designed to be as good as or better than the controls they replace. This mechanism had to be included because, in many cases, it is impossible for a particular organization to satisfy a control as stated in the PCI standard due to

technology or business constraints. Such controls must be in addition to the control already stated within the standard. It is the job of the auditor to determine the efficacy of a proposed compensating control, and whether it can indeed replace a stated control while offering the same level of protection.

Interestingly, an implication of this mechanism allows some flexibility in addressing PCI requirements. It is feasible to imagine a set of "spill-over" effects from various tools that can combine to answer a single requirement. While the requirement is not directly addressed by a specific tool, it is mitigated by the existence of a number of controls employed to address other requirements. Conversely, a single tool can never be considered to "guarantee" compliance; only the auditor is allowed to make that determination.

An example of such a scenario would involve requirement 11.1, which discusses regular testing of access control mechanisms. This requirement seems to be somewhat redundant to requirement 11.2, which requires regular internal and external vulnerability scans, themselves representing a testing mechanism. However, it is feasible to imagine that a tool that continually works to ensure that any in-scope device maintains its desired configuration and operational parameters can provide mitigation for this requirement. Combined with a testing-validation tool that analyses the results of vulnerability scans ("spillover" from 11.2) and removes false positives by automating exploit attempts, this can provide a reasonable overall approach to handling this requirement with relatively low effort.

CONTINUING COMPLIANCE

PCI audits are, as most audits, performed at a particular point in time. They look at a snapshot of an organization's compliance posture at a given time frame—usually a week or two of audit process—and assess overall compliance based on available evidence.

That raises a question: can an audit be passed suc-

cessfully by making a last-minute “rush to compliance,” implementing just enough controls to satisfy audit criteria immediately before the audit takes place?

Indeed, not only is it possible, but it happens frequently. Many organizations work feverishly to the very last minute before an audit begins to create the necessary processes to satisfy requirements. Since initial audits can only examine the existence of these newly implemented processes, but not the evidence of their actual continuing implementation, such efforts are usually crowned with success.

That is, until the second audit.

The main difference between the first and second (and subsequent) audits is that by virtue of being a starting point, the first audit can only examine evidence of the existence of documented process, whereas a second audit can examine evidence of the actual implementation of the documented process.

For example, the auditor must accept your statement that you have implemented a new change management mechanism (PCI section 6.4) upon first audit based on your new change control process documentation. After all, if the process is new, one cannot expect to see its results—yet.

This picture changes during a second audit. Then, the auditor will also expect to see evidence of the change control process actually being followed, in the form of change control tickets, approvals, back-outs and the like. It is no longer possible to simply provide documentation of the process. Now one must also provide evidence of the process being utilized—and in accordance with that same documentation.

The PCI standard has explicit provisions for handling this issue, represented as a significant number of continuing (time-based) audit criteria. These requirements are easy to identify; they usually include words such as “annually” or “quarterly” or “weekly.” As an obvious example, not being able to provide all four quarters of vulnerability scans since the first audit took place is a

surefire way to fail the second, regardless of how stellar the rest of the security infrastructure may be.

Those are the explicitly stated controls. More importantly, PCI also implicitly assumes that pretty much all controls are in place all the time. And in many cases, it is difficult to prove that this is indeed the case. It is for this reason that, from a compliance perspective, controls that can provide continued compliance with the proper evidentiary reporting are worth far more than ones that do not, even if the latter seem to coincide more easily with the point-in-time nature of the audit itself.

Consider system hardening, the topic of the requirements in PCI section 2. It is generally easy to satisfy this requirement during an audit because an auditor is only required to look at a sample of in-scope systems, and those same systems could have been hardened just prior to being examined. However, maintaining systems according to desired hardening settings, especially in a dynamic environment, is not as easy as one might think. Simple carelessness or lack of knowledge on behalf of the administrative staff can easily result in a critical setting or two changing with no realization until it is too late. If that change then results in a breach, and the breach is subsequently tied to the changed setting during the audit that is sure to follow—mandated by the associations and paid for by the compromised entity—then the entity will be deemed to have been non-compliant at the time of breach, and will likely be treated harshly.

How much better would it be if hardening could be continually and automatically maintained? Even better, what if it could be maintained while the system was also automatically maintained from an operational perspective? And what if, on top of such continued maintenance, evidence would be continually produced that could indicate, in a reliable manner, that this is indeed occurring at any given point in time?

From a compliance and audit perspective, tools that provide such functionality are a holy grail. They not only work to ensure that compliance is continually maintained,

but also provide evidence that allows an auditor to determine that the organization has indeed maintained compliance between two point-in-time audits.

TRIUMFANT COMPLIANCE MANAGER

Triumfant Compliance Manager (CM) is designed around the concept of continued compliance. It comes pre-installed with PCI compliance templates that capture all relevant system configuration settings. Triumfant CM is not simply a configuration management tool; instead, it works behind the scenes to continually maintain the system's functionality and healthy operation while keeping it compliant. In other words, desired changes that do not threaten the system's functionality or its compliance are automatically accepted and incorporated into the system's acceptable profile. The strength behind Triumfant CM's engine is in the ability to detect potentially harmful changes—due to malicious software, carelessness on behalf of an admin, or even malicious action by an insider—and automatically correct them without the need for manual intervention.

Note that this approach has some extraordinary and beneficial ramifications. For example, consider that typical Anti-Virus (AV) software generally work off a known database of attack signatures. However, AV products cannot react or indeed do anything to block “zero-day” attacks, those attacks that are too new to have had signatures developed for them yet. With Triumfant CM, an interesting mechanism comes into play; since any malicious software has to impair at least in some fashion the underlying system in order to cause damage, Triumfant CM will notice this impairment and classify it as harmful. It may not realize that it is, necessarily, malware, but it will see it nonetheless. And since the exception will have a direct impact on system functionality, Triumfant CM will be able to reverse it – even automatically, provided the product is configured to act autonomously. Thus it provides a powerful complement to AV systems; what the AV software doesn't catch up-front, Triumfant CM will catch on the back-end. In this regard, Triumfant CM now pushes AV one level higher in the defense-in-depth model,

becoming the “control of last resort” in an organization's security strategy.

Note also that in this regard, Triumfant CM provides “oversight” capability for other types of software. The PCI standard specifically requires that auditors examine the efficacy of existing controls. With Triumfant CM, this efficacy is continually tested; if those controls fail to function properly, Triumfant CM will inevitably see the downpour. And it provides this functionality—automated remediation, continued compliance, and tool oversight—across the entire installed base. Lastly, it does all this with the proper auditing reports to allow auditors to easily be satisfied that not only a chosen sample is compliant over time, but that this is true for the entire environment.

THE BALANCE OF SECURITY AND PRODUCTIVITY

Consider requirement 11.1, where security administrators are required to “Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.” With Triumfant CM working constantly in the background, part of this control is automatically satisfied. Where security controls may and do fail, Triumfant CM will note such failures when they occur as it automatically identifies, assesses and reverses the impact of such failure. In this fashion, Triumfant CM works in conjunction with other security controls to significantly lessen the load on the security administrator, and provides an efficient and automated way to answer at least part of requirement 11.1.

And Triumfant CM does even better. It actually supports the change management control requirements, and doubles up as evidence for the efficacy of those controls. At audit-time, this evidence can be invaluable, as it reinforces the confidence of the auditor in the applicability and implementation of the organization's change control process for systems in scope. Again, Triumfant CM works as a major contributor of supporting evidence for an audit—while at the same time reducing the workload on security and IT personnel.

It is worth noting that Triumphant CM applies equally to workstations and laptops, providing a cost-effective way to continually manage those systems to compliance. Furthermore, Triumphant CM does so without hampering user functionality. End user machines are notorious for being the originators of security breaches, either by virtue of mass infection or simply as an entry point more easily manipulated by malicious agents. And yet, tightening them down too harshly can have a negative effect on an organization’s productivity. Triumphant CM works to deliver a balance between the need for end-point security and usability, allowing users to utilize their PCs in many ways that could be considered dangerous, while seamlessly working behind the scenes to correct any damage they may cause unknowingly – and maintaining their compli-

ance. And of course, much of this balance is achieved without the need for manual intervention from the organization’s helpdesk.

SUMMARY

In summary, compliance is much more than a single deadline. Having tools in place that help maintain compliance on a continual basis will lessen the financial and operational impact that audits generally have on an organization, while helping companies maintain the required safeguards. The ability to prove that such safeguards have existed for the entire duration between audits will both minimize the chance of breach as well as protect the company from liability should a breach occur.

TRIUMPHANT COMPLIANCE MANAGER (CM) AND PCI REQUIREMENTS

In addressing the specific PCI requirements, Triumphant CM may be utilized to perform the following:

- 1.3.9** Allow personal firewalls to be continually managed to desired standard
- 2.1** Examine, report and ensure modification on all vendor-supplied default settings
- 2.2** Continually manage systems to desired and compliant settings while ensuring continued functionality; with pre-defined PCI templates, it can also assess existing compliance posture “out of the box”
- 5.1/5.2** Function as a “control of last resort” preventing the spread of zero-day infections, going beyond AV functionality as well as validating AV effectiveness
- 6.1** Function as a “control of last resort” and validate the performance and effectiveness of the patch management systems as it applies to security patches
- 6.4** Contribute directly to the change control process by managing its own support tickets throughout their entire life-cycle
- 7.2/8.1** Provide supporting evidence in the form of consolidated local machine user listings and roles throughout the installed base

- 8.2/8.5** Validate and enforce many password management requirements for all local users, and can be particularly valuable in environments without a centralized profile management system

- 10.2** Provide supporting evidence for monitoring of several sub-requirements, including for system-level objects

- 10.3** Provide supporting evidence for all sub-requirements

- 10.4** Report and enforce this control for the entire installed base

- 10.6** Alleviate the need for daily log reviews on devices in scope not directly handling cardholder data, as Triumphant CM’s functionality incorporates automated review and remediation

- 11.1** Support this requirement by monitoring the effectiveness of other controls deployed on the system through continued impact analysis

- 11.4** Serve as a host-based intrusion prevention system

- 12.2** Automate some of the tasks in the security operations manual

- 12.9** Support the incident management process by automatically opening and documenting incidents within the change control system