# 10 Tips for a Successful PCI DSS Compliance Project

By **Ashish Thapar** CISSP, CISA, CISM, GCFA, PCI DSS QSA
Professional Services, Verizon Business

**Ashish Thapar** is a Principal Consultant working with Verizon Business in the field of Information Security Consulting. He possesses close to 9 years of rich experience in the field of Information Security spanning across designing, implementing and managing Information Security Management System in large and medium enterprises.

Ashish holds some well recognized security certifications such as CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager) and CISA (Certified Information Systems Auditor). Ashish is also a GCFA (GIAC Certified Forensic Analyst).

Ashish is an accredited PCI QSA (Payment Card Industry Qualified Security Assessor) and PA QSA (Payment Application Qualified Security Assessor). He has been working with Verizon's clients spread across multiple regions to help them strategize their approach to PCI DSS compliance and achieving the PCI DSS certification for their payment card operations.

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to establish minimum security requirements, but there are also best practices that companies can follow to better understand the intent of the Standard, as well as to help provide a smooth implementation. This paper outlines several guidelines on how to achieve a high level of success when performing a PCI DSS compliance project. The tips are not rules, but rather guidelines based on years of industry experience.

The Payment Card Industry Data Security Standard is an industry standard developed to facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a requirement for all merchants and service providers that store, process, or transmit payment card data from one of the participating payment card brands. The participating payment card brands that make up the governing industry body, the PCI Security Standards Council (PCI SSC), include: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

Many companies believe that PCI DSS compliance is a daunting task that is achievable only by big IT spenders. This approach towards compliance does not reflect a fully informed view of the Standard or the strategic approaches towards its implementation. The PCI DSS outlines a procedural approach to compliance by itemizing the 12 "digital dozen" requirements as a checklist. In order to see beyond the audit mentality you must understand several key components of the Standard and how they apply to one's individual business.

While this paper does not propose a *silver bullet* for PCI DSS compliance; it does summarise some key components and approaches that may provide a deeper insight into PCI DSS – to enable compliance.

## TIP 1 – START AS EARLY AS POSSIBLE

One of the common misconceptions about compliance is when to begin planning for the compliance project. Organisations should begin the journey to achieving PCI DSS compliance in the early stages of deciding to accept payment cards or exploring a new acceptance channel; for example moving into accepting payment card transactions online or rolling out a new point of sale (POS) system. Since PCI compliance requires meticulous planning and a well thought out strategy, it is a good idea to start aligning all stakeholders and functional groups necessary to meet this common objective of PCI DSS compliance. There are many examples of companies that ignored PCI compliance in the planning stages of their transaction processing architecture and thus had to face many avoidable issues and fire-fighting. The cost of retrofitting compliance can often be considerably more than proper planning and forethought.

The following are some recommended ways to avoid getting into a *late-starter* mode for PCI DSS compliance:

- Maintain close communications with the business operations staff. Many times a PCI DSS compliance effort is identified and driven due to certain key business objectives. Without the participation of key business executives and the IT staff to properly educate them, the PCI compliance project may get delayed or improperly executed.
- Conduct an internal gap analysis for PCI DSS and make a fair estimation of the key items that are the most difficult or time-consuming to achieve. Understanding those items that require the most time will better enable completion of multiple projects in parallel. For example, if you address the items procedurally, you may not identify requirement 12.8 until the end of the assessment process. This requirement discusses service provider agreements that may take a long time to remediate. Items such as PCI DSS requirement 12.8 should be addressed early in the assessment to help prevent project delays.
- A prioritised approach to PCI DSS is highly recommended, because it helps simplify the process. The prioritised approach that works best may vary from one organisation to another. For example, a large retail organisation may place higher priority on requirements that impact their POS network and retail stores, while a call center may focus on data retention and encryption. Each organisation should prioritise based on their specific environment and systems as well as their appetite for risk (i.e. if you don't tackle a key requirement early on what could be the consequences, and are you willing to accept that risk?)
- It is important to have a trained and experienced professional to help plan the compliance roadmap for the organisation as this can prevent non-compliant architectures, configurations, and potentially unnecessary remediation. If you don't have one in-house, it makes sense to engage a Qualified Security Assessor (QSA) sooner rather than later. Some companies feel they can save money by not engaging a qualified third party until later in the assessment process but invariably this turns out to cost more money – either from under-scoping the PCI effort and then have to re-work it later, or the opposite – over-scoping and having to validate a larger than necessary area.

## TIP 2 – FOLLOW PROJECT MANAGEMENT TENETS: GET A PROJECT SPONSOR, CREATE A CORE TEAM, AND MAKE A PROJECT CHARTER

PCI DSS compliance requires a focused effort. Organisations' effort, time and money is often overspent and may go to waste if all energies are not focused in one direction and led by a robust project management approach.

PCI DSS compliance is indeed a true "project" that must be properly managed. The first step of project management is to verify support from senior management or a project sponsor to confirm the organisations' focus and investment exists to support the compliance effort.

The second step of project management, which is very critical to the success of this project, is to create a formal project charter. This should, at a minimum consist of the following high level sections:

- What initiated the project
- What is being done for whom
- What is the project objective
- What is the project completion criteria
- What are the success parameters
- What is the budget
- What are the major milestones and target dates
- What is in-scope and out-of-scope
- Who are all the stakeholders
- What are the dependencies
- What are the perceived risks and contingencies
- What are the assumptions

The third and very essential step of this process is to develop a core team that has representatives from key stakeholders within the organisation. The responsibility of this core team is to maintain continuous traction and reviews for meeting compliance objectives.

## TIP 3 – LIMIT SCOPE AS MUCH AS POSSIBLE

The scope of PCI DSS compliance is driven by the way cardholder data is being stored, processed, and transmitted at any merchant or service provider. The twelve requirements of PCI DSS apply to all system components. System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. If there is no adequate segregation between the subnets, then the entire network of an organisation becomes in-scope for PCI DSS assessment. Adequate network segmentation can be achieved by implementing firewalls (configured with appropriate access-control lists) between different network subnets.

PCI DSS clearly states that adequate network segmentation which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.

Organisations should always segregate the cardholder data environment to the maximum extent possible. Otherwise the scope increases multi-fold, resulting in increased efforts and timelines much above and beyond the original project estimates.

## TIP 4 – IDENTIFY WHAT IS REQUIRED TO STORE AND DO NOT STORE WHAT IS NOT ESSENTIAL

There is a golden rule in PCI DSS compliance and that is *if you don't need it (i.e. cardholder data, or CHD), don't store it*. Many organisations store too much information that they do not need.

According to the findings of Verizon's 2010 Data Breach Investigation Report (DBIR), 43% of data breaches we investigated revealed at least one type of unknown. One of the prominent unknowns was *"A system storing data that the organisation did not know existed on that system."* This finding emphasizes the importance of knowing all assets and data flow for business operations and disposing of all data that is not needed.

Efforts to achieve PCI DSS compliance increase manifold if any part of cardholder data is being stored unnecessarily. Organisations must objectively evaluate what data is most required for running their business operations. Storage of cardholder data should be kept to a minimum and only that portion which is absolutely required, and cannot be done away with, should be stored. It is important to know what qualifies as cardholder data and consequently what needs to be protected and what is prohibited for storage. PCI DSS v1.2 clearly identifies the security and storage conditions for this data in the section "PCI DSS Applicability Information."

Even if there is a strong business justification for storage of CHD, there are ways to remove the existence of a valid PAN so the data is not within the scope of PCI DSS. For example, a truncated last-4-digit Primary Account Number, or PAN, (xxxx-xxxx-xxxx-1234) is not qualified as CHD. So even if an entity stores cardholder's name, card's expiry date, and card's service code in conjunction with the truncated PAN (as mentioned above), PCI DSS does not apply to this type of data storage. Another method of avoiding storage of CHD could be strong one-way hashing techniques.

There is another type of data that is not permitted to be stored post authorisation, even if encrypted or hashed. This data is called sensitive authentication data. However, there is a misconception amongst some organisations who claim that storing this data post authorisation is required for certain business purposes (e.g. for posting recurring transactions on behalf of customer), avoiding payment conflicts, and charge-back situations. There is no justifiable business reason to store such data post authorisation

## TIP 5 – LOOK BEYOND CHECKLISTS AND TOOLS: FOLLOW THE INTENT BEHIND CONTROLS

Security staff at many organisations tends to look for a readymade checklist or an off-the-shelf tool to simplify their security compliance tasks. What they sometimes forget is that behind the checklist/tool is the real reason for having that control in place.

A checklist or a tool is just one way of providing compliance to a control's objective by a set methodology. While a checklist/tool can provide an organisation with a quick and verifiable method of items being checked, what is more important is to meet the intent of that control in its entirety. At times, a checklist/tool may give a rosy picture, while things might not be as good as they look. So while one may use a checklist/tool, it's important to also apply judgment to determine whether the efforts invested really match the baseline intent of the requirement.

A simple example of this could be a control mandating a stateful firewall to be in place; though in reality the stateful functionality could be switched off due to some legacy applications in use. A checklist based approach to just see whether a stateful firewall is in place would obviously not detect this issue in the implementation of the control.

Another example could be of a control that mandates subscription to essential security updates. If the security staff has merely subscribed to security alerts from vendor websites and are not analysing those alerts and taking necessary actions, then the intent of the requirement is not met and thus all efforts invested are futile.

## TIP 6 – INVOLVE ALL STAKEHOLDERS – COMPLIANCE IS NOT ONLY AN IT MANAGER'S TASK

Achieving compliance with PCI DSS requires involvement from all stakeholders within an organisation. Since it is driven as a formal project, involvement of the project sponsor from business side is imperative. The project team needs to consist of representatives from the information security group, business operations, administration department (of facility services), human resources department, and last but-not-the-least the Information Technology department.

As the 12 requirements of PCI DSS span across different functions within an organisation, active participation of all functions will help maintain compliance with the PCI DSS.

Giving full responsibility for the entire PCI DSS compliance project to an IT manager is highly discouraged and can be a recipe for unexpected delays and over-estimated efforts – and there is a strong reason that this can happen. As PCI DSS is involved with card payments and card payments are a result of some business need, the decisions to forego or limit cardholder data storage, to approve downtime for redesign of network, patch management, penetration testing etc. and to justify business need for storage, processing or transmission of cardholder data are always taken by business executives. These are just some examples of actions that cannot be resolved only by an IT manager. Similarly, controls related to human resources and facility services are to be governed and managed by the respective functions.

It is highly recommended that a core team involving cross-participation from all relevant functions drives the implementation of a PCI DSS compliance project.

## TIP 7 – COMPLACENCY DUE TO COMPLIANCE WITH OTHER STANDARDS COULD BE DETRIMENTAL

PCI DSS is a unique standard that is devised, maintained, and enforced for a very specific reason: protection of payment card data. Although the Standard focuses on best practices in information security, it still needs special attention and focus.

Some organisations are overwhelmed by the level of detail that goes into the PCI DSS. Right from the configuration of key parameters in a firewall, to the key management of encryption/decryption keys, OWASP4 guidelines for application security and up till the quarterly vulnerability assessment, annual penetration testing exercises, the PCI DSS leaves very little scope for assumptions and flexibility while implementing the security requirements.

Often complacency creeps in when an organisation has already implemented other security standards such as ISO/IEC 27001.5 While ISO 27001 is a benchmark standard for information

security from a generic perspective, it is not specifically written for handling risks related to payment card data. PCI DSS's specificity is a differentiator that may require additional effort and at times a change in business practices or technology components for meeting such compliance requirements.

Therefore, even if an organisation is already compliant with another security standard, it should diligently evaluate and conclude additional efforts and/or investments to plan for a PCI DSS project before the last minute rush and chaos. This pre-emptive effort goes a long way in leveraging existing security implementation and being informed about what is already achieved – and what more needs to be done effectively to achieve that *extra bit*.

## TIP 8 – VENDOR COMPLIANCE IS THE KEY

In their focused journey towards PCI DSS compliance; more often than not, organisations forget about the respective compliance of their vendors/ service providers. Compliance of service providers is as important as that of the main organisation, since even when the responsibility of managing certain work involving cardholder data is transferred; the accountability still remains with the main organisation.

PCI DSS is a Standard with a binary compliance outcome, i.e. even if one of the controls is not met, the attempting organisation is deemed as "Not Compliant" to the Standard. There is no term known as "Partially Compliant." It is therefore crucial that an organisation lays equal importance to compliance of their respective vendors/service providers as applicable.

Compliance assessment for vendors/service providers should be done in parallel, without waiting for internal assessments to complete. This is highly recommended, as achieving compliance for the respective control on the service provider's part may entail a complete redesign of the solution implemented, change/upgrade of the product deployed, and/or change management of the contractual terms and conditions. The last one of these is the trickiest and most time consuming affair and may jeopardise an organisation's roadmap of achieving compliance with PCI DSS.

Since the sphere of control for an organisation is limited, confirming service provider compliance with PCI DSS is very important and is critical to drive during the very early stages of an organisation's compliance project.

## TIP 9 – INTERNAL PRE-ASSESSMENTS ARE MORE THAN HELPFUL

Compliance with PCI DSS is not difficult if planned carefully and executed effectively. Before an organisation goes for the final assessment by an external QSA, they should conduct an internal pre-assessment. This is a self assessment exercise, or a mock assessment, where qualified internal resources conduct a PCI DSS assessment in a formal manner and act like an assessor.

An internal pre-assessment is a detailed exercise that helps to identify potential pitfalls and gaps in a structured way. The outcome of this exercise is usually identification of action items, which if remediated in time, make the road to PCI DSS easier.

To conduct this pre-assessment task, an organisation should have qualified personnel who are well versed with PCI DSS requirements and security assessment procedures. These personnel need to conduct this assessment in a formal manner so that the intent, rigor, and structure of an actual assessment are not lost.

## TIP 10 – DOCUMENT WHAT YOU DO AND DO WHAT YOU DOCUMENT

This tip applies universally to any audit, assessment, and certification initiative. Though it's meant to be a very straightforward and simple requirement, this tip is often the most ignored one in many enterprises.

PCI DSS requirements and assessment procedures strongly emphasise evidence of documentation and evidence of implementation effectiveness. These two fundamental requirements are achievable if and only if an organisation religiously documents all implemented controls and maintains implementation of controls as documented.

Matching documentation and execution is critical, as documentation provides repeatability and reproducibility of intent and implementation reflects execution of documented intent. As part of final report submission, a QSA needs to clearly identify what was observed through documentation review, manual checking of implementation effectiveness, and interviews with key stakeholders. Some or all of these procedures need to substantiate an organisation's claim of staying compliant with a particular control within the 12 requirements of PCI DSS.

All documentation should be maintained in a standard manner clearly highlighting the document control information containing, but not limited to:

- Document name
- Document release date
- Document version details
- Document change history
- Document references
- Document author(s), reviewer(s), and approver(s)

A recommended way to ensure that a document stays live as per implementation is to start measuring some Key Performance Indicators (KPIs) for any policy, process, and procedure. This not only helps in measuring and improving a process, it also confirms that the implementation stays close to what is documented and thereby achieves *"Document what you do and do what you document."*

To achieve PCI DSS compliance, an organisation must meet all PCI DSS requirements. This document is meant to be used only for a reference to strategise an organisation's compliance to PCI DSS. ●

## REFERENCES AND ADDITIONAL INFORMATION

About the PCI Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Verizon 2010 Data Breach Investigations Report http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Ten Common Myths of PCI DSS https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

Prioritised Approach for DSS 1.2 https://www.pcisecuritystandards.org/education/prioritised.shtml

PCI Data Storage Do's and Don'ts https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

# The Journal of Financial Services Technology

Published by

**Financial Standard**

a Rainmaker Information company

Level 2, 151 Clarence Street, Sydney NSW 2000 Australia
Telephone (02) 8234 7500 Facsimile (02) 8234 7599
**www.financialstandard.com.au**

**www.jofp.com.au**

## Disclaimer