**PCI Managed Services – A New Approach to PCI compliance from Stickman Consulting**

PCI Data Security Standard is a worldwide acknowledged data security standard that helps organizations develop processes and controls to secure their confidential information, in particular, cardholder data. It states operational and technical requirements and is applicable to any organization that stores, processes and transmits cardholder data. PCI DSS is governed by the PCI Security Standards Council, which was founded by five major card brands i.e. Visa, Master Card, Discover, American Express and JCB. Although for most of the merchants, compliance to PCI DSS seems complicated and frustrating, it indeed saves them a lot of trouble that may result in case of data breach, etc., later on. It also give assurance to credit card companies that their client is taking all possible measures to keep their cardholder data secure. Moreover, the real difficulty is not only to achieve PCI compliance, but also to manage and maintain it as an ongoing process.

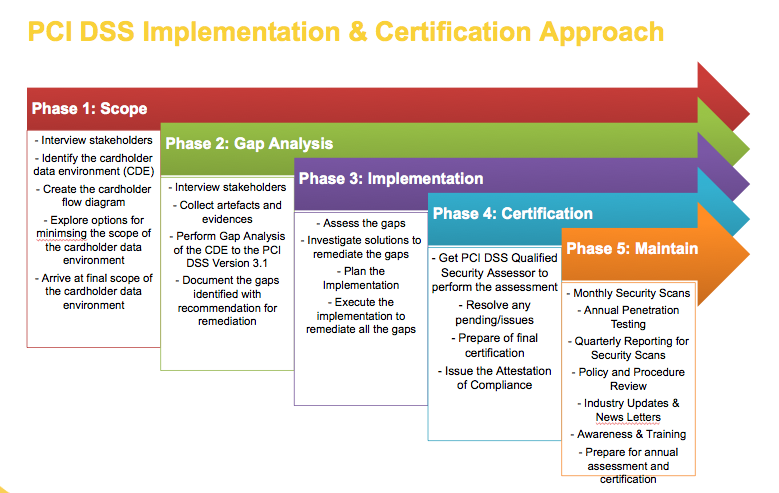
Merchants, especially small merchants, are most vulnerable to threats of data breaches as they are least expected to have taken measures to protect payment card data. According to a research by VISA, level 4 merchants are targeted for payment card information more than 80% of the times as compared to others. Hence, it is equally important for small merchants to achieve PCI compliance as it is for higher levels. Compliance does not only mean that getting an annual certificate can put off all the compliance burden off your shoulders for one year. Rather, it is a continuous process of assessment, remediation and reporting.

**Stickman Consulting – A New Approach to PCI Compliance**

At Stickman Consulting, we strive to provide the best possible services to our clients with a team of qualified and experienced professionals. We have a specialized, comprehensive and practical approach towards PCI DSS services. Our experience in this industry has helped us develop a successful approach to help clients achieve and manage PCI DSS compliance.

PCI DSS compliance programs usually end up at conducting gap-analysis for clients and leaving the remediation task into their hands with little or no practical guidance. Stickman Consulting’s PCI DSS compliance program goes much beyond a mere gap analysis. Usually the clients are presented gap analysis but they do not know what to do with it or how to carry out remediation. PCI remediation itself is a strenuous and time-consuming process and taking this into consideration, our new approach aims to take compliance in our hands right from the start till the end.

Below is a layout of our approach towards PCI DSS as a managed service.



Our service provides a one stop solution to our clients by doing everything for them from scoping and gap analysis to implementation, certification and maintenance. Our structured, proven remediation plan is the need of every business. The following is a remediation roadmap of how we help our clients achieve and maintain PCI compliance with the help of our team of experts and professionals.

1. **Determining what type of PCI DSS compliance is required.**

Your business processes and the transaction volume of your cardholder data indicates what “type” of PCI DSS compliance does your organization need. PCI SSC provides different kinds of Self-Assessment Questionnaires or SAQs that help with the initial assessment. Depending upon the level of your organization, our team will help you self-assess or provide an actual onsite Level 1 assessment as a Qualified Security Assessor (QSA).

1. **Conducting initial gap analysis.**

After the identification of a required and suitable SAQ or onsite Level 1 assessment, we help you conduct a thorough gap analysis that is based upon requirements of the appropriate SAQ or according to complete PCI DSS standard for Level 1 onsite assessment.

1. **Dividing remediation tasks into various categories:**

Not everyone is good at everything. Therefore, it is important to categorize remediation tasks and assign accordingly. For example, gaps in policies and procedures are remediated by someone who is experienced in technical writing. Similarly, misconfigured servers are looked upon by someone who is expert in operating systems and applications.

1. **Determining the requirement of any new tools, products, etc.**

Now that remediation tasks have been categorized, we determine what exactly needs to be done to put the remediation to work. For areas where you may not have time to work or may not have the required technical experts, we bring in new tools, products and most importantly, new manpower. Remediation often revolves around the development of policies and procedures and technical issues such as hardening, audit trails, logging, and implementation of monitoring tools like File Integrity Monitoring, etc.

1. **Remediating and Testing**

We set a remediation time frame for ourselves and go accordingly. Also, tests are conducted to check that all components in scope are meeting the standard requirements. Moreover, because compliance is an ongoing process, it is in our practice to provide an annual checklist to the client.

**How Can we Help You with our Remediation Services?**

* Stickman Consulting provides assistance to its clients for developing and implementing an Information Security Program to achieve and maintain compliance in accordance with PCI DSS. This includes awareness sessions, policies, procedures, vulnerability management, risk management program, etc.
* Our security awareness training sessions will educate the biggest weakness of the organization in terms of its information security, i.e. the employees. We provide regular training sessions to employees, managers and other staff to keep them aware about latest security issues and PCI DSS changes.
* Our vulnerability management service aims to address the issues of identifying vulnerabilities, scanning, patching and risk rating.
* Our security monitoring services include file integrity monitoring, audit logging, IDS monitoring, ad A/V monitoring.
* Our security testing service allows regularly and scheduled testing of the service to ensure compliance. Security tests include penetration testing, vulnerability scanning, web application security testing and wireless security testing.
* Stickman Consulting’s incident response plan is effective and states procedures for responding to potential or already incurred suspected incident in accordance with PCI DSS. Our team also trains the staff on incident response and tests the incident response plan according to PCI DSS.

Below is a table that briefly illustrates how Stickman Consulting provides PCI Compliance as a managed service to its clients in accordance with the requirements of PCI DSS.

|  |  |  |
| --- | --- | --- |
| **Requirement No.** | **Requirement** | **Stickman Consulting’s Remediation Steps** |
| **Build and Maintain a Secure Network** | | |
| 1. | Install and maintain a firewall configuration to protect cardholder data | * Executing, evaluating and optimizing custom-built firewall * Developing and implementing standard documentation |
| 2. | Do not use vendor-supplied defaults for system passwords and other | * Conducting penetration tests and vulnerability scans * Developing and managing vulnerability management program * Developing and implementing standard documentation |
| **Protect Cardholder Data** | | |
| 3. | Protect Stored Cardholder Data | * Implementing and managing Data Loss Prevention * Implementing and managing Access Management * Implementing, managing and testing Business Continuity and Disaster Recovery plans |
| 4. | Encrypt transmission of cardholder data across open, public networks | * Implementing, evaluating and optimizing encryption mechanism |
| **Maintain a Vulnerability Management Program** | | |
| 5. | Use and regularly update anti-virus program | * Evaluating and implementing anti-virus software * Implementing and managing Access Management |
| 6. | Develop and maintain secure systems and applications | * Managing Application Security Program and reviewing code |
| **Implement Strong Access Control Measures** | | |
| 7. | Restrict access to cardholder data by business need-to-know | * Evaluating organizational security policy and procedures * Creating user awareness regarding security policy and procedures * Implementing and managing Access Management |
| 8. | Assign a unique ID to each person with computer access | * Evaluating and implementing security tools that administer access control |
| 9. | Restrict physical access to cardholder data | * Conducting information security awareness sessions * Training and testing against social engineering |
| **Regularly Monitor and Test networks** | | |
| 10. | Track and monitor all access to network resources and cardholder data | * Designing and implementing log management, IDS/IPS and File Integrity Monitoring * Evaluating and implementing Access Management * Providing assistance with policy and procedure management |
| 11. | Regularly test security systems and processes | * Conducting regular vulnerability scans and penetration tests |
| **Maintain an Information Security Policy** | | |
| 12. | Maintain an Policy that Addresses Information Security | * Developing, implementing, updating information security policy |