COMP307 CW #3: Align Compliance Requirements to PCI DSS

Kevin Ma – 300867968

Thursday, November 15, 2018

After reviewing the “For Merchants” link on <https://www.pcisecuritystandards.org/merchants/>, answer the following questions:

# What are the PCI DSS compliance requirements?

There are 12 PCI DSS compliance requirements. They are as follows:

|  |  |
| --- | --- |
| GOALS | PCI DSS REQUIREMENTS |
| Build and Maintain a Secure Network | 1. Install and maintain a firewall configuration to protect cardholder data  2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data  4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software or programs  6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need-to-know  8. Assign a unique ID to each person with computer access  9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for employees and contractors |

# Which organizations should be PCI DSS compliant?

PCI DSS applies to all organizations involved in payment card processing. This includes merchants, processors, acquirers, issuers, and service providers. In addition, PCI DSS also applies to all other organizations that store, process, or transmit cardholder data and/or sensitive authentication data.

# What is the purpose of the PCI DSS Security Audit Procedures?

The purpose of the PCI DSS Security Audit Procedures is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews, so that software vendors can validate that a payment application complies with the PCI DSS Payment Application Data Security Standard (PA-DSS).

# What is the process for obtaining the PCI DSS Compliance?

Validation of compliance with the PCI Data Security Standard is determined by individual payment brands. All have agreed to incorporate the PCI Data Security Standard as part of the technical requirements for each of their data security compliance programs. The payment brands also recognize qualified security assessors and approved scanning vendors qualified by the PCI Security Standards Council. The Council does not enforce compliance; this is done by individual payment brands or acquiring banks.

Separate and distinct from the mandate to comply with the PCI DSS is the need for entities to verify and demonstrate their compliance status. It's a fundamental and critical function that identifies and corrects vulnerabilities and protects customers by ensuring that appropriate levels of cardholder information security are maintained.

For example, for MasterCard, their process is as follows:

* 1. PCI Self-Assessment
  2. PCI On-site Assessment
  3. PCI Network Scanning
  4. PCI Payment Applications

This process would be different for other payment card brands:

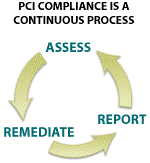
* American Express
* Discover
* JCB International
* Visa
* Visa Europe

However, they tend to follow the general trend shown below with some additional steps depending on the organizations:

1. Analyze your compliance level (self-assessment)
2. Fill out self-assessment questionnaire
3. Make any necessary changes to your business
4. Find a provider that uses data tokenization to secure customer’s credit card information
5. Complete a formal attestation of compliance
6. File the paperwork and submit to payment card organization

# What are 3 (steps) for adhering to the PCI DSS?

Many organizations treat compliance as a one-time, annual event. But only focusing on an annual compliance assessment can create a false sense of security. However, PCI Compliance is a continuous process. An entity needs to:



* **Assess**
  + Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.
* **Remediate**
  + Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.
* **Report**
  + Compiling and submitting required reports to the appropriate acquiring bank and card brands.

# How does VISA define the levels of the PCI DSS Compliance?

Merchant levels as defined by Visa:

|  |  |
| --- | --- |
| Merchant Level | Description |
| 1 | Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. |
| 2 | Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year. |
| 3 | Any merchant processing 20,000 to 1M Visa e-commerce transactions per year. |
| 4 | Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year. |