NOVEMBER 1, 2022

PCI DSS: ACHIEVING FINANCIAL DATA SECURITY

WHITE PAPER BY AUUDITR

Introduction

With the advent of electronic money transaction systems, vulnerabilities also increased. Data systems, transaction modules, applications, and databases became more mature, but so did the risk of online theft and financial damage. Data breaches with credit card tracking and financial credentials increased along with the online market and merchandise scope.

Payment Card Industry Data Security Standard (PCI DSS) tackles merchant-based vulnerabilities and gives a system for financial data security. The card processing system includes the following:

- Point of sale devices
- Mobile devices/ Computer systems
- Wireless access points
- Online shopping
- Remote access connections

PCI DSS covers the vulnerable ends and makes the cardholder’s data more secure. This standard applies globally where the entities store, process, or transmit sensitive information.

This standard is governed by PCI Security Standards Council, founded by American Express, JCB International, MasterCard Worldwide, VISA Inc., and Discover Financial Services. The standard comprises best security practices to achieve data protection and clients’ trust.

We shall further discuss the contents of this standard and Auuditr’s services to help companies achieve compliance.

> “Data breaches with credit card tracking, and financial credentials increased along with the scope of online market and merchandize. "

Keywords: Cardholder Data, PCI DSS, Visa, MasterCard, JSB International, Auuditr, Cyber Security, Financial Data Security,

Context and structure

> “PCI DSS applies to all businesses working to store, process or transfer the cardholder data. "

PCI DSS is a security guideline to ensure the maximum data protection of cardholders. This standard works on three basic principles:

1. **Assess** – Identification of the locations of cardholder data, analyzing IT assets and business processes to find vulnerabilities in operational and technical aspects.
2. **Repair** – The vulnerabilities found are now fixed, and any unnecessary storage or step from the process is removed.
3. **Report** – The assessment and fixation remedies are now documented, and reports are submitted to the banks, card companies, or any other requesting entity to inform them about your current security state.

PCI DSS applies to all businesses that store, process, or transfer cardholder data. The standard has a set of requirements particular to the type of business:

- **PCI Pin Transaction Security or PTS** is for manufacturers who majorly work with PIN Entry Devices. It works with the Point of interaction (POI) Modular Security and Hardware Security Module (HSM). These requirements are for the manufacturers to design, develop and transport the device to the user.
- **Payment Application Data Security Standard (PA DSS)** deals with vendors who develop software and payment applications that store, process, and transfer cardholder data.
- **PCI Data Security Standard** builds and maintains a secure network system, follows a vulnerability management program, and regularly monitors the networks for loopholes.

PCI DSS requirements are further discussed in detail here:

1. Build and maintain a firewall to protect the data.
2. Encrypt the transmission of cardholder data in public networks to protect the data.
3. Protect the systems against malware and maintain a program for early detection of vulnerabilities in systems and applications.
4. Control the physical and logical access to the cardholder data. Restrict where access is not required.
5. Regularly monitor and test the security systems and processes.
6. Maintain an Information Security Policy.

Services Offered by Auuditr

As a consultancy firm, we offer our team the expertise to develop processes and management methods to ensure information security in organizations. We provide the following services:

- Gap assessment sessions to find out the existing capability of the organization
- Policies and procedure guidelines
- Selection of applicable SAQ (Self-Assessment Questionnaires)
- ROC (Report on Compliance)
- Consultancy sessions

Auuditr works with the validation tools offered by the standard and helps the clients to assess and follow the set of requirements. We also provide consultancy sessions for the further management of information security within the organization.

Further information on

www.Auuditr.com