DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

ICT DIVISION
FUTURE IS HERE

Bangladesh Computer Council

BGD e-GOV CIRT

Simplifying PCI DSS

[Payment Card Industry Data Security Standard]

Simplifying PCI DSS (Payment Card Industry Data Security Standard)

Foreword

The aim of this write-up is to assist organizations that store, process, communicate or otherwise handle credit or debit card data in understanding; how the PCI DSS applies to them; and what the requirements of the standard are. One of the myth about PCIDSS "PCI DSS is too hard". Understanding and implementing the 12 requirements of PCI DSS can seem daunting; especially for merchants without a large security or IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI DSS compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations.

Here, basics of PCIDSS requirements and highlighting of few those requirements are now a days followed by most small, medium or large IT organization or business organizations.

Write-up objectives

- ➦ Highlighted few important requirements to understand the framework more easily.
- ➦ Typical payment card risks faced by organizations and basic knowledge to address few basic risk.
- ➦ Golden rules for protecting cardholder data.
- ➦ Scope and structure of the PCI DSS.
- ➦ The importance of segmenting the CDE (Cardholder Data Environment).
- ➦ The 12 high level requirements of PCI DSS.
- ➦ Interfacing with ISO/IEC 27001.

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
1 Router & Firewall	Review of configuration rule(s) sets at least every six months	Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts	Follow Change Process	Maintain Network Diagram specially Cardholder Data Environment (CDE) and data flow across system	Establish Role & Responsibility Matrix
2 Do Not Use Vendor Supplied default Password	Change defaults/remove unnecessary default accounts	Develop configuration standards	Use strong cryptography	Maintain an inventory	
3 Protect stored cardholder data	Limit cardholder data storage and retention time	Do not store sensitive data after authorization	Mask PAN (Primary account number) when displayed. the first six and last four digits are the maximum number	Do not store the personal identification number (PIN)	Do not store the card verification code (three-digit or four-digit number printed on the front or back of a payment card used to verify, after authorization.

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
4 Encrypt transmission of cardholder data across open, public networks	Use Strong cryptography and security protocols: Only trusted keys and certificates are accepted	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	The use of WEP, SSL as a security control is prohibited	ASV (Approved Scanning Vendor) Quarterly (3)	
5 Protect all systems against malware and regularly update anti-virus software or programs	Deploy anti-virus software on all systems (particularly personal computers and servers)	Ensure that anti-virus programs are capable of detecting, removing, and protecting	All anti-virus mechanisms Are kept current	Generate audit logs which are retained per PCI DSS Requirement 10	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users.

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
6 Develop and maintain secure systems and applications	Establish process to identify security vulnerabilities	Protect system and software from vulnerabilities	Critical Security Patches apply within 1 Month	Follow change control processes and procedures	Develop applications based on secure coding guidelines (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.)
7 Restrict access to cardholder data by business need to know	Level of privilege required (for example, user, administrator, etc.) for accessing resources	Access control system(s) that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed	Level of privilege required (for example, user, administrator, etc.) for accessing resources	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
8 Identify and authenticate access to system components	Remove/disable inactive user accounts within 90 days.	Immediately revoke access for any terminated users. Failed attempt (Lock user) = 6, New passwords cannot be the same as the four (4) previously used passwords	All users a unique ID. Passwords/phrases must meet the following: 1. Minimum length of at least seven (7) characters. 2. Contain both numeric and alphabetic characters	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Set the lockout duration to a minimum of 30 minutes. Change user passwords/passphrases at least once every 90 days.
9 Restrict physical access to cardholder data	Use appropriate facility entry controls to limit and monitor physical access	Video cameras or access control mechanisms (or both) to monitor sensitive areas	Classify media so the sensitivity of the data can be determined.	Maintain strict control over the storage and accessibility of media	CCTV data need to retain 3 month

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
10 Track and Monitor all access to network resources and cardholder data	Protect audit trail files from unauthorized modifications	Promptly back up audit trail files to a centralized log server or media that is difficult to alter	Review at least daily: 1. All security events 2. Logs of all systems that store, process, or transmit *CHD and/or *SAD 3. Logs of all critical system	Retain audit trail history for at least one year, with a minimum of three months available for analysis	Follow up exceptions and anomalies identified during the review process
11 Regularly test security systems and processes	Perform quarterly internal vulnerability scans	Run internal and external network vulnerability scans at least quarterly	Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV)	Penetration testing at least annually and after any significant infrastructure or application upgrade	Wireless 3 Month log check

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
12 Maintain a policy that addresses information security for all personnel	Establish, publish, maintain, and disseminate a security policy	Review the security policy at least annually	Implement a risk-assessment process at least annually	Service Provider activity monitoring Annually	Monitor and control all access to data

Legend:

1. CHD- Cardholder Data
2. SAD- Sensitive Authentication Data

Written By

Muhammad Moinul Hossain
M.Sc., CISM, CISA, ISO ISMS LA, ITIL, ENSA
IT Auditor
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council