Introduction

# Management plan

A payment card industry data security management plan is a properly written and designed process that ensures secure management, storage, and transmission of payment card data inside an organization. The plan lets in an outline to keep compliance with the PCI DSS requirement. The management plan constructs steady surroundings for clients' secure payment environment by combining key factors, including risk assessment, security coverage strategies, access controls, encryption measures, and reporting. Overall, it minimizes the potential for data breaching and maintains the framework of a responsible custodian.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Requirement | | PCI REQ (IF APPLICABLE) | INITIAL COST | ANNUAL COST | INITIAL COST | ANNUAL COST |
| HARDWARE | | | | | | |
| Firewall for the office | | 1.1,1.2,1.3 | $2000 | $100 | $1200 | $50 |
| Firewall for wireless LAN | | 1.2.3 | $1000 | $50 | $0 | $0 |
| Layer 3 Switch | | 1.3,11.3 | $1000 | $50 | $750 | $50 |
| Physical security | | 9.3 | $2000 | $0 | $1000 | $0 |
| Video surveillance | | 9.1.1 | $5000 | $500 | $3000 | $250 |
| SOFTWARE | | | | | | |
| Antivirus | 5.1,5.2 | | $200 | $200 | $100 | $100 |
| Personal firewalls | 1.4 | | $200 | $200 | $100 | $100 |
| Total |  | | $12500 | | $6500 | |

The above table illustrates the ROI ( returns of investment) associated with the PCI DSS implementation compliance. Implementation of the P2PE encryption security has proven to be effective in results. According to the table, a 48% overall decrease in cost was achieved in the organization's annual and initial costs. An important note is that this data was taken from various sources on the internet. The result may differ depending on the various geographical locations or in certain scenarios based on the organization.[1]

# Explanation of the official document

PCI DSS v4

The PCI Security Council officially released version 4.0 of the PCI data security standard on March 31, 2022. The newer version of the PCI DSS is crucial in providing a foundational guideline to technological and operational criteria to safeguard account-related data. PCI DSS v 4.0 announces different updates and versions to bring important updates to the standard. Following the PCI DSS v4.0, training accessories can conduct the required assessment using the v4.0 or previous version suitable for the need. Moreover, the late version offers space for implementing time frameworks and standard requirements, offering the organization flexibility and adaptability.

To adapt to the dynamic and evolving security landscape of the business environment within the payment sector, it is a necessity that security implementations must be continuously updated and adapted accordingly. Notable improvements have already been introduced: strict multifactor authentication MFA specifications, updated password requirements, and new guidelines addressing e-commerce and malicious activities to combat the current environmental issues. Further, the newer version is equipped with specific role-based responsibilities for individual requirements, aiding in communicating clear instructions for better understanding establishing and maintaining security. An updated reporting mechanism was introduced. The overall development in the areas provides charity for security report reviewing and proves a continuously dating and enhancing security practice.

Introducing new standards to encourage innovation in payment technology and expanding the variety of ways companies can meet their security objectives. These standards include access to the public, shared, or user groups accounting introduced targeted risk assessment chapter Also, in verification methods Processes are also enhanced, with verification methods and response to it goes deeper there. This ensures a close match between the data collected during compliance validation and the information in the compliance report or self-assessment questionnaire. This new data gives companies more flexibility and advanced wear tools to intensify their security efforts in the ever-changing payment technology landscape.[2]

# Self-assessment questionnaires

Questionnaire A

This applies to retailers who accept orders through telephone or online channels and use a third party to manage the collection, storage, and processing of cardholder data when the retailer's systems do not handle cardholder information processing or transmission in particular. This includes establishments that only accept card payments when a physical card is used. A third party responsible for these functions must follow the payment card Industry Data Security Standard (PCI DSS) to ensure proper handling of cardholder data.[4]

Questionnaire A-EP

This choice is only accessible to online sellers. In this situation, the seller has arranged with a third-party service provider to handle the processing of card payments processing, similar to self-assessment questionnaire A. The security of the payment process impacts the seller's website. The third-party provider must adhere to the PCI DSS.[5]

Questionnaire B

Vendors use printers or dial-out interfaces instead of storage media payment card data. This is because the card data device will not have an internet connection. It does not apply to online services. In this case, the merchant usually keeps only receipts. It can include cardholder information.[3]

Questionnaire C -VT

This option is intended for business owners using virtual terminals in a web browser without storing cardholder information. In this case, a PCI DSS-compliant service provider may be responsible for performing a remote installation or virtual payment application. Because the virtual terminal doesn’t directly connect to card data, businesses manually enter cardholder information into the system during payments.[6]

Questionnaire C

This policy applies to business owners and retailers who use online payment systems but do not store digital cardholder data. An internet-based processing system on occurred transactions processes cardholders' data. The related data of the cardholder is not stored digitally, increasing security and reducing data breaches.[7]

Questionnaire P2PE

This option does not apply to online merchants, as it is intended for companies using point-to-point encrypted payment terminals. The Payment Card Industry Data Security Council must approve the payment processing system. This method is considered more straightforward than the other methods by allowed conditions. In this case, merchants collect money from customers in person, usually through physical point-of-sale transactions.[8]

Questionnaire D

This option is available to vendors and business owners who do not have the requirements for another self-assessment form. It is also used by service provider companies that provide payment card services to other businesses.[3]

# PCI DSS complaint Checklist

The payment card industry data security standards (PCI DSS) include 12 criteria an organization must overlook to achieve compliance with the standards. [9] These cities are organized into six distinct “control goals” objectives that serve as the main pillars for improving the protection of cardholders' data. These goals hold various information aspects of the cardholders' related data, which involves strengthening network security, enabling IT security policies, and addressing vulnerabilities. The overall progress not only strengthens the security of the cardholder data but also enhances and contributes to development in cybersecurity and IT risk management.

Based on the company's needs, recommendations are carried out for specific environments and levels of compliance. Furthermore, a general understanding of the control goals and requirements is needed to grasp the core principles of implementing PCI DSS, providing and safeguarding cardholder data and security within the payment industry.

A table with text on it

Description automatically generated

Figure pci security standard quick overview

References

References

[1]

Bluefin, “The ROI and TCO of a PCI-Validated P2PE Solution,” *Bluefin*, Feb. 23, 2017. https://www.bluefin.com/bluefin-news/roi-tco-pci-validated-p2pe-solution/ (accessed Oct. 27, 2023).

[2]

secuirty standerd council, “Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0,” 2022.

[3]

The Diligent team, “PCI DSS compliance explained,” *Diligent.com*, 2021. https://www.diligent.com/resources/blog/pci-dss-compliance-explained

[4]

“Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire A and Attestation of Compliance Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced,” 2014.

[5]

“Payment Card Industry Data Security Standard Self-Assessment Questionnaire A-EP and Attestation of Compliance For use with PCI DSS Version 4.0,” 2022.

[6]

“Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire C-VT and Attestation of Compliance Merchants with Web-Based Virtual Payment Terminals -No Electronic Cardholder Data Storage For use with PCI DSS Version 3.2 Revision 1.1,” 2017.

[7]

“Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire C and Attestation of Compliance Merchants with Payment Application Systems Connected to the Internet- No Electronic Cardholder Data Storage,” 2014.

[8]

“Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire P2PE and Attestation of Compliance Merchants using Hardware Payment Terminals in a PCI SSC-Listed P2PE Solution Only -No Electronic Cardholder Data Storage For use with PCI DSS Version 3.2,” 2016.

[9]

“PCI Compliance Checklist for 2022,” *Secureframe*. https://secureframe.com/blog/pci-compliance-checklist (accessed Oct. 27, 2023).