ASTANA IT UNIVERSITY

Report

Assignment 4

Student of group: CS-2115N

Full name: Adil Ergazin

Tutor: Zhanshuak Zhaibergenova

Astana 2023

Assignment 4

Objectives

Part 1. PCI DSS checklists preparation analysis

Part 2. PCI DSS checklists preparation results

Background

There are 12 different PCI compliance requirements that covered entities must follow in order to handle credit card information in a secure matter. Failure to follow these requirements greatly increase your company's chance of hacking, fraudulent activity, or data breach.

1. Implement firewalls to protect data
2. Appropriate password protection
3. Protect cardholder data
4. Encryption of transmitted cardholder data
5. Utilize antivirus software
6. Update software and maintain security systems
7. Restrict access to cardholder data
8. Unique IDs assigned to those with access to data
9. Restrict physical access to data
10. Create and monitor access logs
11. Test security systems on a regular basis
12. Create a policy that is documented and that can be followed

Part 1. PCI DSS checklists preparation

Here is a quick PCI compliance checklist for you to get started:

1. **Understand which compliance level applies to your business**

   Sample:

PCI Compliance Level	Annual Transactions
Level 1 (High Difficulty)	Over 6 million
Level 2 (High Difficulty)	1 - 6 million
Level 3 (Moderate Difficulty)	20,000 - 1 million
Level 4 (Low Difficulty)	Fewer than 20,000

Selected compliance level :

PCI Compliance Level	Annual Transactions
Level 4 (Low Difficulty)	Fewer than 20,000

According to the previous assignment about losses and damage in 25 million tenge related to personal information, it was calculated considering the number of users was about fewer than 20, 000. Furthermore, on account of that, the Level 4 (low difficulty) compliance level was selected for this project.

2. **Have protocols and processes in place for privacy and compliance**

   As the web application related to notes, by considering the necessity in providing payment transitions, it will contain a subscription feature to obtain and update their privileges, such as the ability to possess "to do" lists and other aspects associated with them.

   But the project consists of FTP, HTTPS, TLS, Kerberos and others based on the presence of an Active Directory. It also has a Firewall at each endpoint.

3. **Establish accountability within the organization**

   For accountability, the organization possesses an administrator of web application and system administrator.

4. **Provide compliance training for employees**

   The compliance training would be provided for 7 days and confirmed at the end of the training week.

5. **Appoint a Data Protection Officer (DPO)**

   To do data protection officer stuff, the two employees would be appointed (sys admin, cybersecurity specialist).

6. **Regularly test your security systems**

   The several test operations would be covered in 3 stages of testing (3 audits) twice per week.

7. **Have a response plan in the case of a data breach**

   In the case of data leaks, 25 million is planned to be spent; additionally, 2 million is in the budget of any situation.

8. **Enforce both physical and technical safeguards**

   The physical safeguards based on server holding place are in the safety location and under the supervision of sys admin administrator, with technical safeguards in addition.

9. **Ensure your security policy is up to date**

   Our security policy is updated each day upon network component improvements and also technically in Active Directory.

10. **Understand the full scope of all cardholder data without assumption through the use of a data discovery tool**

    Depending on payment transactions, they would be supported with Kaspi or other banks, but the cardholder data won't be saved; only the history of subscription purchases will be in individuals' payment histories, and they will be enclosed with the SHA-256 hash function in the database.But also the transactions wiill be protected with TLS/SSL protocols.

Part 2. PCI DSS checklists preparation results

PCI OBJECTIVES	PCI REQUIREMENTS (V4.0)	RESULTS
Build and maintain a secure network and systems.	1. Implement firewalls to protect data 2. Appropriate password protection	1. Firewalls to each point 2. Block chain baised SHA-256 hash function
Protect cardholder data.	3. Protect cardholder data 4. Encryption of transmitted cardholder data	3. Encrypted history with SHA-256 hash function 4. TLS/SSL protocols
Maintain a vulnerability management program.	5. Utilize antivirus software 6. Update software and maintain security systems	5. Windows Defender 6. Active Directory regularly updates, Wazuh SIEM system
Implement strong access control measures.	7. Restrict access to cardholder data 8. Unique IDs assigned to those with access to data 9. Restrict physical access to data	7. Administrator only 8. Active Directory features 9. Sys Administrator only
Regularly monitor and test networks.	10. Create and monitor access logs 11. Test security systems on a regular basis	10. Wazuh SIEM system 11. 3 varieties of audits twice per week
Maintain an information security policy.	12. Create a policy that is documented and that can be followed	12. Policy based on Adilet laws and ISO 45001 standards

Report

In this assignment of confirming PCI DSS (Payment Card Industry Data Security Standard) compliance, the project must be checked by 12 checklists, and it should be greater than 70%. By observing the PCI DSS checklist table, the requirements were split into six general objectives:

- Build and maintain a secure network and systems (by first two checklists)

- Protect cardholder data (by next two checklists)
- Maintain a vulnerability management program (by next two checklists)
- Implement strong access control measures (by next three checklists)
- Regularly monitor and test networks (by the penultimate two checklists)
- Maintain an information security policy (by the last one checklist)

The results revealed, by the analysis of checklists, the possibility of security of cardholder data might rely on these 12 requirements. In order to compute the compliance of a web application project, there are all requirements, beginning with 100 percentages divided into checklists with 6 generalized objectives defined at 16.66% per PCI aspect instead of the “Protect cartholder data” part with a significant weight of 16.7%. Further, each PCI aspect would be divided by the number of included requirements. If concentrate focus to the computation processes, in the first objective, by considering the first requirement, it will be 8.33, and the next will also be 8.33; by subtracting them, it will be declared at 16.66%. By relying on the significance of the next PCI objective, it must be computed carefully, and by dividing it into two checklists, it would be 8.35% per checklist. In the “Protect holder data” segment, the third requirement is known as the most protective hash algorithm, rated at 8.35%, and the next TLS/SSL is rated at the same 8.35% in addition, concluding 16.7% in outcome. If we focus on the next part, in the “Maintain a vulnerability management program” part, by exploring the first checklist of antivirus software, Windows Defender, it will be 50/50 secure, then it will be half of 8.33%, or exactly 4.165%. And the second checklist was rated at 8.33% for its remarkable system of updating software and managing security systems. By moving to the next element of PCI objectives, in the “Implement strong access control measures” element, the first and third checklists will vary based on the fact that physically and technically, cardholder data access will be allowed to only one individual for each responsibility and by dividing 16.66% to 3 checklists both of two checklists will be rated 5.44%. But on account of the importance of the second one, which might impact others, the two checklists will be rated at a maximum of 5.45%. In the next part of “Regularly monitor and test networks," the beginning step was rated at 8.33%, relying on the effectiveness and strength of testing methods by three varieties of audits, such as scientific and industrial audits, expert audits, and system audits, but the next one was rated at 4.165% depending on regulated by including the human factor that for monitoring provided only one cybersecurity specialist who will monitor occasionally. In the final generalization of “Maintain an information security policy”, the last step was rated at 16.66% on account of being precise and matched with laws and standards globally and locally.

In conclusion, observing all outcomes of each mapped part, which included the first at 16.66%, the next at 16.7%, the third at 12.495%, the fourth at 16.66%, the penultimate at 12.495%, the

last at 16.66%, and the PCI DSS compliance result was evaluated at **91.63%** by adding all objective scores. Hence, this project might be certified by PCI DSS.