ASSIGNMENT 4

Theme: PCI DSS checklists preparation

The Payment Card Industry Data Security Standard (PCI DSS) is a global security requirement for any organization that processes, stores or transmits credit cardholder information

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

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

1. Understand which compliance level applies to your business
2. Have protocols and processes in place for privacy and compliance
3. Establish accountability within the organization
4. Provide compliance training for employees
5. Appoint a Data Protection Officer (DPO)
6. Regularly test your security systems
7. Have a response plan in the case of a data breach
8. Enforce both physical and technical safeguards
9. Ensure your security policy is up to date
10. Understand the full scope of all cardholder data without assumption through the use of a data discovery tool

https://www.strongdm.com/blog/pci-compliance-requirements by using this link check 12 requirements of your project.