**Overview of PCI DSS**

Payment Card Industry Data security standards were initiated to encourage and enhance the payment card data and keep it consistent by adopting security measures globally. Nowadays we use payment cards all over the places such as point of sale devices, mobile devices, online shopping, banking and where not. It’s become a serious crime as more that 900 million people with sensitive information have been affected due to the fraud with payment cards and hence PCI DSS came to the rescue and made it imperative to adapt the security procedures and technologies to protect the data.

**PCI DSS Compliance is the continuous process:**

1. **Access**: Recognizing all areas of cardholder information, taking a stock of your IT resources and business forms for installment card handling and examining them for vulnerabilities that could uncover cardholder information.
2. **Repair**: Fixing the identified vulnerabilities, safely evacuating any unnecessary cardholder information, and executing secure business forms.
3. **Report**: Documenting evaluation and remediation points of interest, and submitting consistence reports to the obtaining bank and card brands you work with or the service provider.

**PCI Requirements:**

To overcome the breaches and frauds the PCI Security Standards Council (PCU SSC) have set some technical and operational requirements to protect the card holder data. PCI DSS globally applies to all the organization that store, process and transmit data or have sensitive authentication information about the data. The council is responsible to set the security standards. There are 12 requirements of the PCI DSS, one of them is explained in detail below:

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

Firewall are the devices which control the traffic in and out of the organization’s network. It can give us access to the most secured areas and components of the organization. The hardware and software used in connecting different networks are in scope of this requirement. A firewall can examine all the network traffic and allow only those who meet the specified security criteria.

The below measures should be taken to overcome the vulnerability caused due to firewall configuration.

1. Establish and implement firewall and router configuration standards: Firewall and routers are the main components of the architecture to control the access to the data.

Configuration standards will help to make sure that the first line of defense (firewalls) will remain strong.

1. The process of approving and testing all the network connections: This process will help in solving the misconfiguration of the network, router and firewall. The formal process can be followed to prevent problems while configurations. Without the approval of the changes, the system cannot be updated which could lead to inconsistency between network documentation and actual configuration.
2. Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks: Without the network diagram the device could be overlooked and detail information about the card holder data will be compromised. The diagram can show the flow of data with the network and hence give us the opportunity for enhancements and improvements.
3. Restrict inbound and outbound traffic and only allow traffic specific to cardholder data and deny the rest: This will help to restrict malicious activities inside the network. It will also help to fic the loop hoes which gives a back door for the hackers to hack the data.
4. Non-disclosure of private IP addresses and routing information to unauthorized parties will help and prevent from hackers using and fake IP address to access the network.
5. Restrict the portable computing devices used to process card holder data to be only used inside the company’s network to avoid internet frauds and threats.
6. All the security policies, documentations and operational procedures are well documented and are in use by all the parties to have knowledge and transparency within the system.