The Payment Card Industry Data Security Standard requirements vary depending on the method of credit and debit card processing being used. The different methods are defined in the Self-Assessment Questionnaires (SAQ) as follows:

- **SAQ A: All Cardholder Data functions outsourced. No Electronic Storage, Processing, or Transmission of Cardholder Data**
  - The organization does not store, process or transmit any Cardholder Data on organization systems or premises but relies entirely on a third party service provider to handle these functions.
  - The third party service provider handling storage, processing, and/or transmission of Cardholder Data is confirmed to be PCI DSS compliant.
  - The organization does not store any Cardholder Data in electronic format.
  - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.

- **SAQ B: Imprint Machines or Standalone Dial-out Terminals Only, No Electronic Cardholder Data Storage**
  - The organization uses only an imprint machine to imprint customers’ payment card information and does not transmit Cardholder Data over either a phone line or Internet, or,
  - An organization uses only standalone, dial-out terminal which is not connected to the Internet or any other systems within the organization environment.
  - The organization does not store Cardholder Data in electronic format.
  - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.

- **SAQ C: Payment Application Connected to the Internet, No Electronic Cardholder Data Storage**
  - The organization has a payment application system and an Internet or public network connection on the same device.
  - The payment application system is not connected to any other system within the organization environment.
  - The organization’s store is not connected to other store locations and any network is for a single store.
  - The organization does not store Cardholder Data in electronic format.
  - If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.
  - The organization’s payment application software vendor uses secure techniques to provide remote support to the organization’s payment application system.

- **SAQ C-VT: Web-Based Virtual Terminal, No Electronic Cardholder Data Storage**
  - The organization’s only payment processing is via a virtual terminal access by an Internet connected web browser.
  - The organization accesses the virtual terminal via a computer that is isolated in a single location, and is not connected to other locations or systems within the organization’s environment.
  - The organization’s virtual terminal solution is provided and hosted by a PCI DSS validated third party service provider.
  - The organization’s computer does not have software installed that causes Cardholder Data to be stored.
o The organization’s computer does not have any attached hardware devices that are used to capture or store Cardholder Data.

o The organization does not receive or transmit Cardholder Data electronically except through the virtual terminal.

o The organization does not store Cardholder Data in electronic format.

o If the organization does store Cardholder Data, it is only in paper records or copies of receipts and is not received electronically.

- SAQ D: Electronic Storage of Cardholder and Service Providers

  o All other organizations not meeting the requirements of a SAQ A, SAQ B, SAQ C or SAQ C-VT in addition to all service providers. This includes all organizations that retain Cardholder Data.