**Context establishment**

Prior to start implementation of PCI DSS, context establishment and defining scope must be done.

Before scoping,

* Availability of inventory data
* Accurate identification pf card data and card data storage locations
* Inputs from all stakeholders such as vendors, application developers, database owners etc.

Must be confirmed available in order to expect a higher successful implementation of PCI DSS.

There are 3 main categories of scoping when implementing PCI DSS.

**PCI DSS scoping contains**

1. People scoping
2. Process scoping
3. Technology scoping

**Data and systems that applies PCI DSS**

* Systems that process, store, or transmit card holder data
* Systems that provide security services to card holder data
* Systems that are connected to card holder data
* Systems that may impact the card holder data environment

Few examples for the categories of scoping are provided in this document.

**1. People scoping**

* Cashiers
* Call center operators
* system administrators
* Database administrators
* Application developers
* Customer support employees
* Information security related employees

**2. Process scoping**

* Payment processing channels (ATM, POS, Ecom, MOTO)
* Reconciliation, Settlement processes
* Reporting
* Log management
* System hardening
* Incident management
* Access controlling

**3. Technology scoping**

* Servers
* Network devices (Routers, Switches)
* POS devices
* Remote access systems
* Application software
* Security solutions
* Laptop/ Desktop PCs

By considering all these categories and related entities, a complete scope for PCI DSS can be created.