PCI DSS compliance: A closer look at Requirements 1.1.2 and 1.1.3 – Cardholder Data Environment Diagrams

January 2018

What is a Cardholder Data Environment?

At its simplest, an organisation's Cardholder Data Environment (CDE) is the physical and technical environment where Account Data is being accepted, captured, handled, processed, stored and/ or transmitted. Anywhere that people, processes, and technologies store, process, or transmit Account Data will be in scope for the Payment Card Industry Data Security Standard (PCI DSS) and considered part of the CDE.

As most card data breaches involve a compromise of the CDE, PCI DSS requirements require a wide variety of security controls to be maintained to help protect this data on its entry into, when it is within and on its exit or removal from the CDE.

The CDE consists of:

- All system components that store, process, or transmit Account Data;
- Systems components that do not in themselves store, process, or transmit Account Data but are 'adjacent to' (e.g. on the same network as) a system components that do.

However, the PCI DSS applies to more than just the system components within the CDE; also in scope are 'connected-to or security-impacting' systems components that:

- Connect or have access to the CDE either directly or indirectly, e.g. via a jump server;
- Can impact the configuration or security of the CDE, e.g. server providing name resolution (DNS) for the CDE;
- Provide security services to the CDE, e.g. identification & authentication server, such as Active Directory;
- Support PCI DSS requirements, e.g. audit log server;
- Provide segmentation of the CDE from out-of-scope systems, e.g. internal firewalls.

For additional guidance on determining whether systems are in scope or out of scope, please see the articles referenced below.

System components can be network devices, servers, computing and mobile devices, and applications. That may include but is not limited to;

- Virtualisation components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances
- Server types such as web, application, database, mail, proxy, etc.
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications
- Third party devices, systems, networks or people, such as remote access, VPNs, IT support.

What is Account Data?

Account data, also often referred to as Payment Card Data, is comprised of Cardholder Data (CHD) and Sensitive Authentication Data (SAD):

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

From PCI DSS v3.2 page 7

CHD and SAD must be protected as per the PCI SSC guidelines:

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment. Organizations should contact their acquirer or the individual payment brands directly to understand whether SAD is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.

---

2 Sensitive authentication data must not be stored after authorization (even if encrypted).
3 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere
4 The three- or four-digit value printed on the front or back of a payment card
5 Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message

From PCI DSS v3.2 page 8

Why do I need a Cardholder Data Environment diagram(s)?

The creation of network and data flow diagram(s) that define the CDE (Cardholder Data Environment diagrams) is one of the most important first steps for any organisation trying to determine Account Data use across their people, locations, functions, processes and systems and hence to define their PCI DSS assessment scope. The CDE diagram(s) should be used as one of the organisation's central reference sources when addressing with PCI DSS compliance and protecting Account Data.

Network and data flow diagram(s) are required by the PCI DSS:

PCI DSS Requirement	Guidance
1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Network diagrams describe how networks are configured, and identify the location of all network devices.
1.1.3: Current diagram that shows all cardholder data flows across systems and networks	Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network.

Organisations required to formally assess their compliance must have network and data flow diagram(s). For self-assessing entities, a network diagram is mandatory for the PCI DSS SAQ A-EP, SAQ B-IP & SAQ D questionnaires, while the SAQ A-EP and D also requires a card data flow diagram. For the remaining questionnaires, these diagrams are not mandatory but it is good practice to create one or more diagram to illustrate the CDE, the network(s) and systems that are part of or connect to the CDE and the journey of CHD and SAD across systems and network(s), as it is captured, transmitted, processed and potentially stored. Without the diagrams, Account Data may be overlooked, unprotected, exposed to fraud, or stored in breach of PCI DSS.

By understanding where Account Data is captured, transmitted, processed and / or stored, it can;

- Help an organisation understand and define its CDE.
- Define the PCI DSS assessment scope.
- If applicable, identify the relevant PCI DSS SAQ questionnaire/s.
- Help determine which PCI DSS requirements are applicable to the organisation.
- Highlight potential security weaknesses in networks/systems/processes.
- Highlight potential opportunities for reducing the scope of the PCI DSS assessment

How to create a Cardholder Data Environment Diagram

To identify where Account Data storage, processing, or transmission is within your organisation, it is necessary to understand all payment method/channels. This is a generally a collaborative effort between departments, potentially also involving third party service providers, and can be broken down by the three payment channels – Ecommerce, Face-to-face, and MOTO (Mail Order/Telephone Order).

To develop a CDE diagram you will need;

- **Up-to date IT network documentation**
  Without a current network diagram, systems could be overlooked, and unknowingly left out of the security controls implemented for PCI DSS, or network connections could be left poorly protected that could leave the CDE vulnerable to attack or compromise by malicious individuals.
- **Knowledge of all Account Data handling and payment processes within the organisation**
  Gather information on all aspects of account data receipt, capture, processing, retention/storage, archiving and destruction. This must include not only card payment processes but also account data handling processes such as bookings (where card data is captured but no payment taken), chargebacks, refunds, etc.

  You will need to identify all of the people (including third parties), processes and technologies involved in the handling/transmission/processing of account data (in both hard copy or electronic form) across all teams, functions and services involved in each payment method/channel. This is often the most difficult part to investigate due to the many different forms, and historic ways of taking account data throughout an organisation.

The first step to creating a CDE diagram is to document what is and isn't included in the CDE.

Follow the movement of the account data from its entry point(s), through the organisation until it permanently leaves the organisation or is destroyed. This will identify all the components that are involved in the processing, storage, and transmission of the cardholder data.

For merchant organisations, mapping the list of Merchant Accounts or Merchant ID's (MIDs) to each payment channel can help to identify payment processes and card data flows. Note that not all MIDs may be used to process payments directly by the organisation. Some MIDs may be used by third parties to process payments on the merchant organisation's behalf. The merchant retains responsibility for the protection of account data and fulfilment of the applicable PCI DSS requirements by third party service providers and must therefore include those activities when defining assessment scope and creating CDE diagram(s).

Steps to creating a Cardholder Data Environment Diagram

1. Create or use an existing network diagram showing all locations, networks, and connectivity (internal and external).

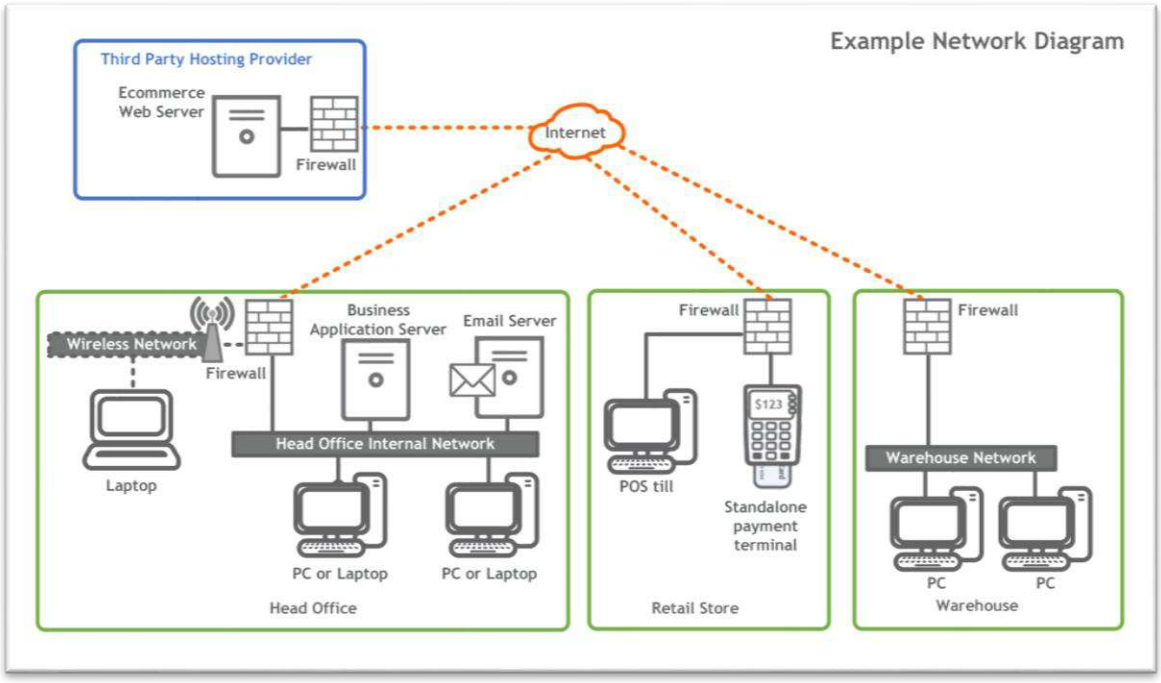
   A hand drawn diagram is the best place to start, and can be made professional using a design package. Due to requirement 1.1.2(b) requiring the diagram to be updated when changes occur, a design package makes it easier to make revisions and create a version history.

   There are many different design packages that can be used to draw the diagram, some free, some expensive, all with different functionality.

   Here are a selection;

   - Microsoft Visio
   - Gliffy
   - Draw.io
   - LucidChart
   - yEd

   An example of a basic network diagram;



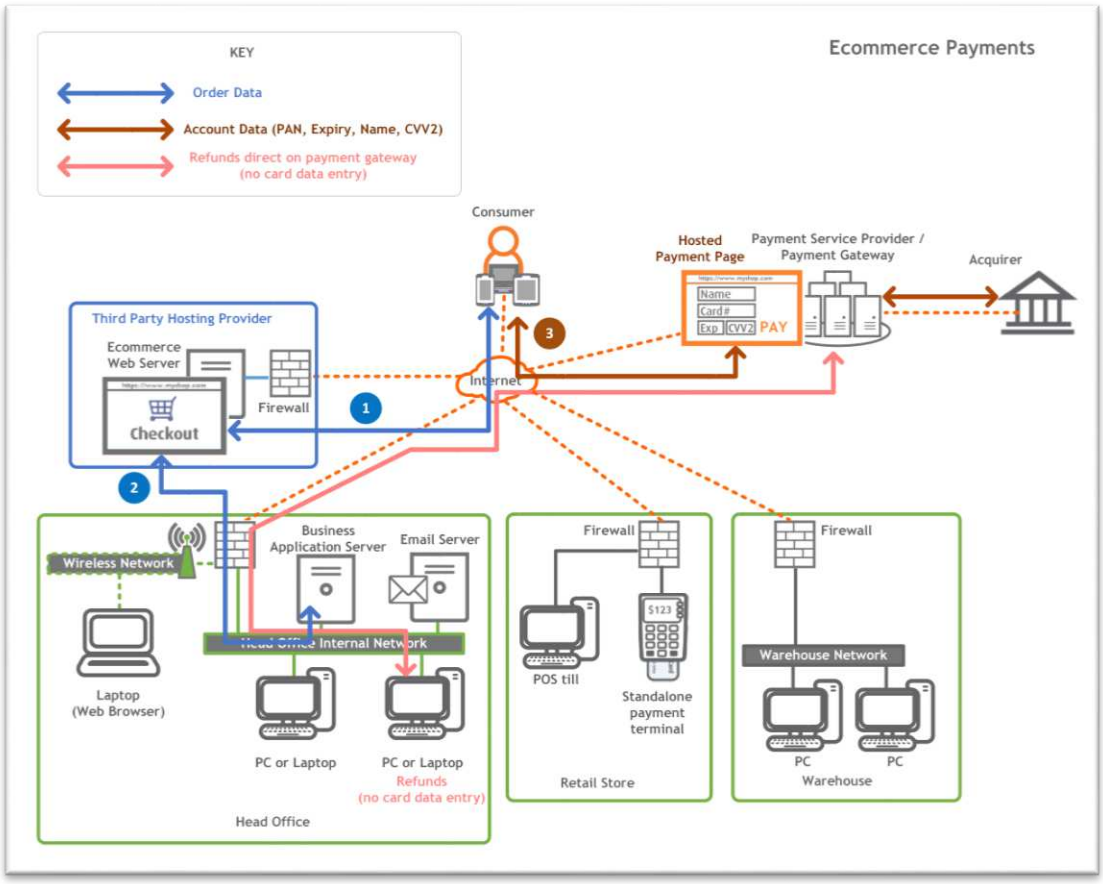
2. Create a copy of the network diagram for each payment channel that is used – Ecommerce, Face-to-face, and MOTO. A single diagram can work for smaller configurations but may become confusing with multi-channel environments.

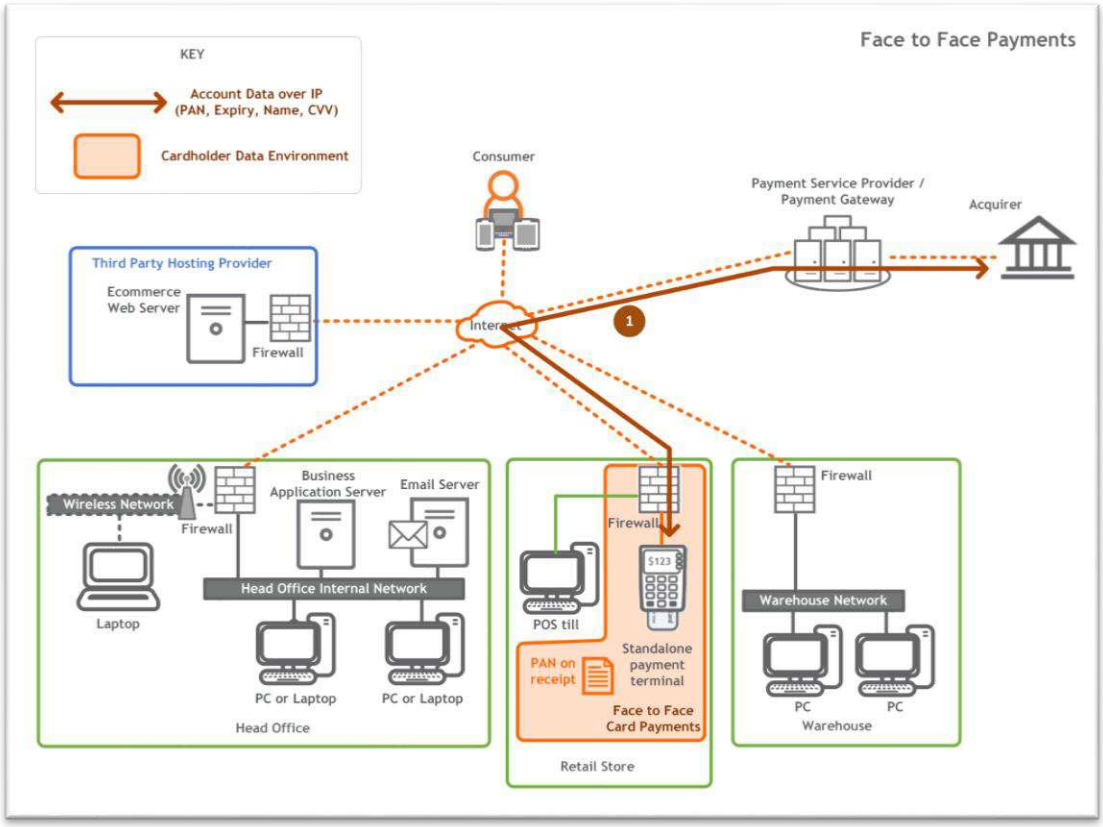
3. Add payment systems that store, process, or transmit CHD (per the guidance in 'What is a Cardholder Data Environment') for each payment channel to the diagrams.

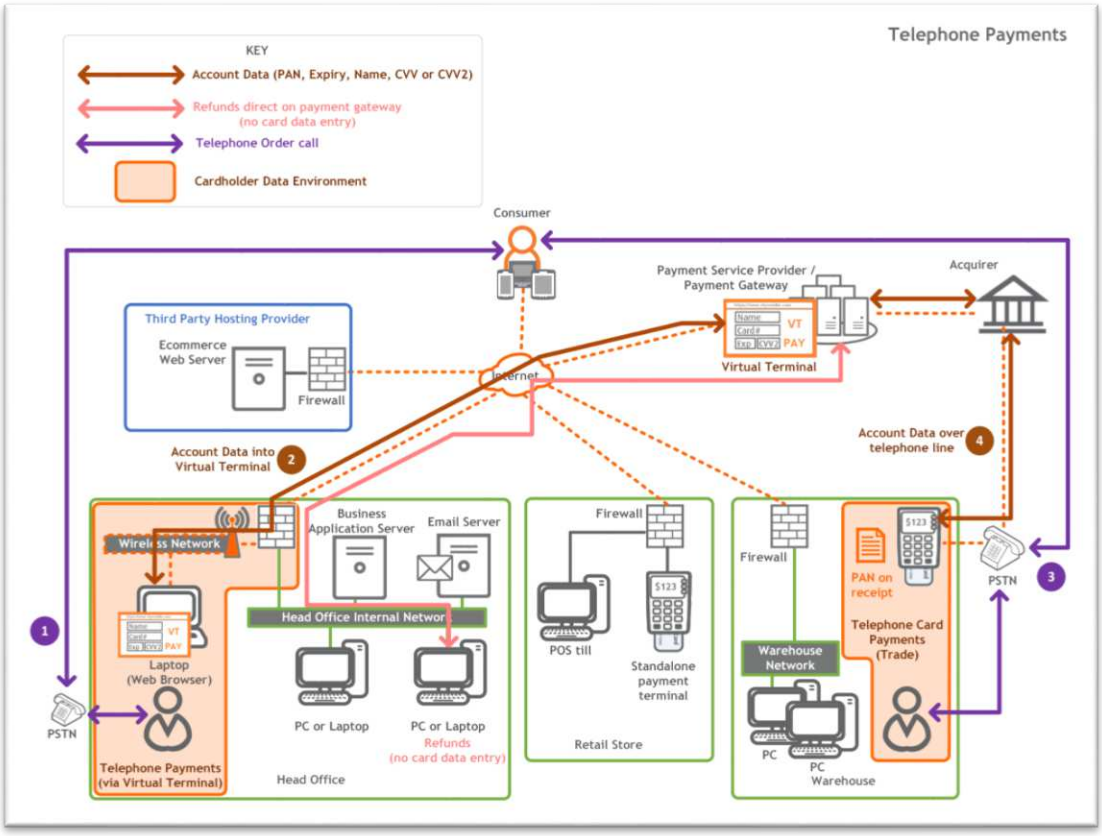
   Examples would be;
   - Websites hosted internally or by a 3rd party service provider
   - Applications/databases
   - Payment terminals (PSTN, network (IP), or mobile (GPRS)
   - Virtual terminals
   - POS systems (PC's, servers, equipment)
   - Telephone call recording systems
   - VOIP telephone systems
   - Post/email
   - Merchant receipts/paper
   - Fax/e-fax
   - Backup systems/sites/devices/media
   - Archived cardholder data/systems
   - 3rd party devices/systems/support

4. Use arrows and numbers to show the cardholder data flow movement between people, devices, people, and entities as shown in the simplified examples below. In addition, use colour coding and keys to assist in showing where CHD is;
   - Stored
   - Processed
   - Transmitted
   - Encrypted
   - Unprotected

Payment channel CDE diagram examples







References

- PCI DSS v3.2
- PCI SSC Guidance for PCI DSS Scoping and Segmentation
- Sysnet New PCI SSC Scoping & Segmentation Guidance: What does it mean?