PCI Resources - PCI DSS Scoping Model and Approach

Source: http://www.pciresources.com /pci-dss-scoping-model-and-approach/

The approach and model described here are excerpted from Volume 2 (PCI DSS Scoping) of the PCI Resources book series covering the PCI DSS. Details of the analysis that led to this model, and of other relevant scoping details, can be found in that volume (mostly section 2.5). While PCI DSS Scope covers the people, processes and technologies (PPT), this model will detail mostly the technology portion, the IT system components. People and processes involved should also be covered by organizations.

This model and approach is available under a creative commons licence: Attribution-ShareAlike CC BY-SA (see details on the last page).). The volumes in the book series are the intellectual property of their owners and not distributed under this licence. This model approach is the result of Yves Desharnais' thinking and experience with PCI DSS since 2012 (version 2.0). This model is not endorsed or approved by the PCI SSC or anyone else.

It is my hope that opening this model will help everyone agree on what should be in scope, or at least have a reasonable basis for classification and discussion. I believe that this model could also be applied to other data requiring protection, for example, patient health information (PHI) or personally identifiable information (PII). The December 2017 update to version 1.2 of this model aligned with the May 2017 PCI DSS Information Supplement from the PCI SSC and called "Guidance for PCI DSS Scoping and Network Segmentation v1.1" (this supplement will be referred to as the "May 2017 Guidance". This model was updated to reflect the language changes to PCI DSS 4.0 during summer 2022. No substantive changes were made, only visuals were updated, and clarifications added.

Acronyms

In this model and approach, you'll see me use many acronyms, which I define here:

- Account Data = the complete set of data covered by the PCI DSS, and composed of both CHD and SAD
- CHD = Acronym for "Cardholder Data"; consists of the full PAN, and in the presence of full PAN, cardholder name, card expiration date, and/or service code
- PAN = Acronym for "Primary Account Number"; the unique card number (credit, debit, or prepaid cards, etc.) generally printed on the front of the card.
- SAD = Acronym for "Sensitive Authentication Data", it includes the full track data (from magnetic stripe or equivalent on a chip), the PIN or PIN block, as well as the card validation verification codes/values (often referred as CVV2 but can take any of the following acronyms depending on card brands: CAV2/CVC2/CVV2/CID).
- SPT = An acronym for "Store, Process, or Transmit", meaning that a system or process comes into contact with CHD and/or SAD and is therefore automatically in scope.
- CDE = Acronym for "Cardholder Data Environment", basically what we are trying to protect, which starts with the systems that SPT Account Data (CHD or SAD), or have unrestricted connectivity to these.
- Isolation = There is no possible access between systems.
- Controlled Access = There are limited (restricted and strictly controlled) communications possible between systems.

- RoC = Acronym for "Report on Compliance" - the report format of a full audit used to document detailed results from an entity's PCI DSS assessment.
- Entity = An entity is any organization that has the responsibility to protect account data; for PCI DSS compliance, an entity will generally be defined as either a merchant or a service provider.
- DESV = PCI DSS Designated Entities Supplemental Validation for PCI DSS 3.2.1, v3#3.1, a new PCI standard released in June 2015 which is now integrated as appendix A3 of 3.2

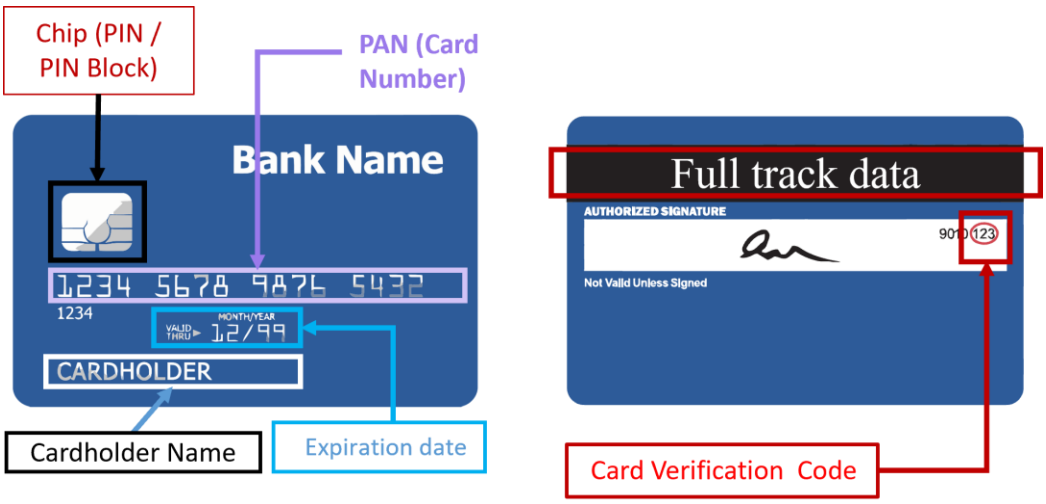

Figure 1 - Rendering of Payment Card (Front and Back) with data elements identified

Scoping categories

My approach to scoping (developed in 2014), as other approaches do, is used to categorize systems. I initially defined three (3) basic categories that are derived directly from the language of the PCI DSS standard: CDE, connected and out-of-scope. One issue I have with the PCI SSC Guidance on scoping regards whether segmentation devices (or combinations thereof) constitute CDE systems (my initial contention) or connected systems (PCI SSC, and OPST); I have thus decided to treat segmenting devices as their own category, which I will explain in the revised model. This has no effect on scope, simply on clarity. I'll describe these one-by-one, starting from the inner core that we are trying to protect: the area where we have CHD and/or SAD, the CDE. As for any model including mine, I advise following the adage attributed to statistician George Box: "All models are wrong, but some are useful".

First Category: CDE systems

All CDE systems are often called category 1 or type 1 devices. There are 2 different sub-categories in the CDE, but all applicable requirements will apply to all CDE sub-types equally. FAQ #1252 responds to the question "*Do all PCI DSS requirements apply to every system component?*" It starts with: "*PCI DSS requirements apply to all system components, unless it is has been verified that a particular requirement is not applicable for a particular system*". We'll refer to this FAQ in volume 3 when discussing how to address each of the requirements.

<u>CDE/CHD</u>

As stated earlier, the scope definition in PCI DSS 4.0 was updated based on the May 2017 Scoping Guidance, and this is now clearer than its previous location (page 10 of PCI DSS 3.2.1). It now starts with a definition of the CDE which aligns perfectly with this model.

PCI DSS requirements apply to:

- *The cardholder data environment (CDE), which is comprised of:*
  - *System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and,*
  - *System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.*

The first sub-bullet is our first category.

All these systems that SPT CHD/SAD are part, or form the basis, of your CDE (Cardholder Data Environment - the core environment in scope for PCI). We'll refer to these as CDE/CHD systems. The May 2017 Scoping Guidance refers to these as "[s]ystem component stores, processes, or transmits CHD/SAD". The OPST calls these type "1a".

CDE/Contaminated

The second sub-bullet of the new scope definition identifies our second sub-category.

- System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

In the network segmentation section, the standard states that*"[s]egmentation (or isolation) of the CDE from the remainder of an entity's network is not a PCI DSS requirement"*. Therefore, network segmentation is not required other than at the external perimeter of the network. The standard also adds: "[w]ithout adequate segmentation (sometimes called a 'flat network'), the entire network is in scope for the PCI DSS assessment". If you do not use segmentation, everything is subject to PCI DSS requirements. Basically, your CDE expands to all systems that are in the same network as your in-scope CDE/CHD systems described above until some segmentation prevents it.

We shall call these systems in the same network zones as CDE/contaminated since there could easily be a transfer of information between systems that are not otherwise restricted (generally by a firewall or other device). The May 2017 Scoping Guidance refers to these systems as *"[s]ystem component is on the same network segment (for example, in the same subnet or VLAN) as system(s) that store, process or transmit cardholder data"*. The OPST calls these "1b".

Second category: Segmenting (previously called CDE/Segmenting)

The second major category are systems that provide the (generally network) segmentation and prevent "contamination" of CDE systems via some form of "controlled access". Typically, these are firewall devices, but they are not limited to those (more so now with the renaming of firewall to Network Security Control, or NSC, in requirement 1 of PCI DSS 4.0). These devices are called Segmenting systems. The segmentation section of the scope definition includes an instruction to that effect (and present in previous PCI DSS versions): "[i]f segmentation is used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment". This is covered by requirement 11.4.5, v3#11.3.4.

Note that this function may be accomplished by a combination of devices and systems, but the more complex this gets, the better the documentation your assessor will require.

In the OPST, these would be either "1b": or "2a", thus leading to potential confusion. Without segmenting systems, we cannot have connected systems. The PCI SSC May 2017 Scoping Guidance calls these "[s]ystem component segments CDE systems from out-of-scope systems and networks". They place those systems in the connected systems category ("Connected-to or Security-impacting Systems") which, in my opinion, can lead to confusion. This is why I mark these as a separate category to to prevent any confusion. This is my only major disagreement with the PCI SSC document.

This second category is furthermore warranted by the inclusion of a new requirement since PCI DSS 3.0 regarding the testing of segmentation during the required annual internal penetration tests (11.4.5, v3#11.3.4). Section 3.2 (Segmentation) of the 4.0 RoC template adds documentation of this validation of adequate segmentation was performed. Note that the network access control (e.g. firewall) rules that are unrelated to the CDE environment would be out-of-scope. This could happen if the firewall manages the connection point between the CDE and various other network segments. In that case, only the rules that pertain to access to the CDE are in-scope (for review), although it would be a good idea to treat all of them in the same way.

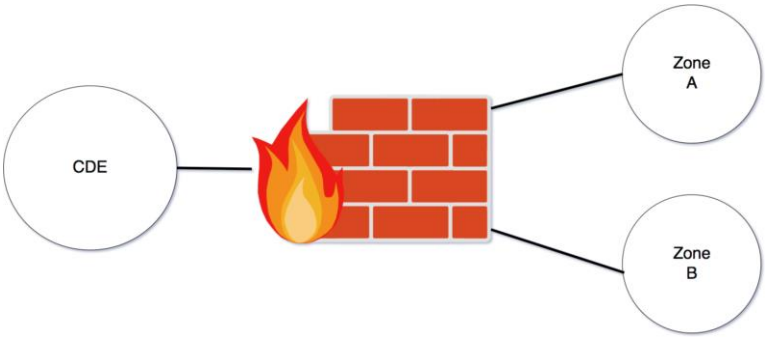

Figure 2 - Image of firewall and 3 network zones (including the CDE)

For example in the diagram above, the rules that limit zone A to zone B connections would be out-of-scope.

Whichever solution is chosen to provide segmentation (physical firewall, virtual firewall, virtualization technology, etc.), entities should provide an annual evaluation that covers requirement 11.4.5, v3#11.3.4 demanding segmentation penetration testing (every 6 months for service providers with 11.4.6, v3#11.3.4.1).

Segmentation in virtualization and cloud computing

The "PCI DSS Cloud Computing Guidelines" supplement covers segmentation in sections 4.4 through 4.4.3. It clearly states: "Segmentation on a cloud-computing infrastructure must provide an equivalent level of isolation as that achievable through physical network separation." Although cloud computing is mentioned, this is also the litmus test for any virtual environment. So an organization must "ensure that their environment is adequately isolated from the other client environments. In terms of clouds or hosting providers, that assurance is made by the provider, whereas in internal environments this would be validated by the organization. Ultimately however, responsibility that validation has been performed (by someone) rests on the organization.

In section 4.4.1, the recommendation is made to use a "dedicated CDE hypervisor" to simplify the issue of segmentation (which is made more complex in cloud environments than in private hosting). Dedicating the hypervisor to the CDE systems (no mixed-mode) is also what many QSAs I've spoken to use as minimal guidelines.

Third category: Connected systems

After the CDE scope definition (first bullet and its two sub-bullets) of PCI DSS 4.0, another bullet preceded by the word "AND" is added, defining the connected systems (presented below). The PCI SSC includes segmentation in the connected systems category but I prefer to treat them as separate, as just explained.

So when does a CDE system contaminate another? Some cases are easier to understand than others. For example, if two systems are in the same network segment and can communicate more or less freely (depending on opened services) then it is clear that contamination can occur (note that the possibility is sufficient to warrant inclusion). But what is required for a "connected" system not to become contaminated? Let's break it down to figure it out.

We know that communication between CDE and connected systems must be restricted to only those services required for business operations (called "controlled access") according to requirements 1.3.1, v3#1.2.1-inbound and 1.3.2, v3#1.2.1-outbound. Now, we can't always keep all systems we need inside a single zone, or we would be defeating the goals of scope reduction that we should aim for. So what are we to do in these instances?

The 2nd bullet of the scope definition identifies those systems not completely isolated from the CDE. The standard includes in scope any "[s]ystem components, people, and processes that could impact the security of the CDE". This is further addressed on multiple occasions in the 2013 RSA presentation and the 2013 PCI community meetings presentation:

> *If it can impact the security of the CDE, it is in scopeRemember non-CHD systems may be in scope too*

and

> *If an "out-of-scope" system could lead a CDE compromise, it should not have been considered out of scope*

Thus, if we are unsure whether or not a system is in scope (as a "connected" system), we should look at whether a compromise of the system could lead to an attack on a CDE system without needing to first compromise another system. If that is the case, then this system is in scope. The second subtype of connected systems will partly address this as well.

In this methodology, we use isolated to indicate that two systems cannot communicate at all with each other. If communication is limited (note: use of the "any" or "generic" rules are prohibited in PCI DSS), we call it controlled access. The RSA conference presentations confirm this:

- *To be out of scope: segmentation = isolation = no access*
- *Controlled access ≠ isolation*
- *Controlled access:*
    - *Is still access*
    - *Is a PCI DSS requirement*
    - *Does not isolate one system/network from another*
    - *Provides entry point into CDE*
    - *Is in scope for PCI DSS*
        - *Verify access controls are working*
        - *Verify the connection / point of entry is secure*

Connected systems are often referred to as category 2 or type 2 devices. As in the CDE case, there are different types of "connected" devices that present a different level of risk. Connected systems are generally represented in **yellow**. Let's examine those three subtypes.

Connected/Security

There are systems such as user directories (Active Directory, LDAP), patch management systems, vulnerability management systems, several others (this is not an all-inclusive list) which provide 'security services'. We can call these connected/security systems.

The May 2017 Guidance for PCI DSS Scoping and Network Segmentation creates 3 categories of systems that I consider as Connected/Security in a section they call "Connected-to or Security-impacting Systems":

- System component impacts configuration or security of CDE
- System component provides security services to the CDE
- System component supports PCI DSS requirements

I consider that all these types of systems were included initially by my model, but the added clarification from the PCI council is welcome. Those categories are also found on figure 1 on page 13 of the PCI DSS 4.0 standard.

The OPST calls these "2a".

Connected/Communicating Systems

Any system that is 'connected to' the CDE (or has a connection to systems in the CDE) is considered a 'connected' system. The exception are systems on the 'outside' of Segmenting systems, for example when a Segmenting also affects traffic not related to the CDE such as that described in the Segmenting section and presented in Figure 2.

Some connected systems (that have a connection to CDE/communicating systems) may eventually be ruled out-of-scope, but an evaluation must be formally documented by the organization to determine if PCI DSS applies. It could be a system receiving information outside the CDE with no possibility of re-entry. For example, say that we have a connected system that receives periodic information transfers initiated from a CDE system and that we have ensured that no CHD/SAD is transmitted. The protocol used for data transfer is sftp (part of the SSH suite of applications). The traffic is initiated from the CDE, a file is uploaded to the connected system, and then the connection is closed. Other than returning status messages as part of the protocol, there is no information flowing back to the CDE system. I would contend that the connected system as described here could be ruled out-of-scope since it cannot have an impact on the security of the CDE (although some DLP tool may be warranted on the system initiating communication). Documentation of the evaluation process should be created, maintained and kept, to be presented to your assessor. The May 2017 Scoping Guidance refers to these when a "[s]ystem component directly connects to CDE". The OPST calls these "2b" for incoming or "2c" for outgoing based on who initiates communication; in contrast to the OPST, I don't make the distinction based on flow-direction, but on details of communication and protocols used.

Connected/Indirectly

There are also systems that do not have any direct access to CDE systems (they are isolated from the CDE) but that are still in scope. Instead, they would generally have access to other connected or

segmenting systems and, through these, could affect the security of the CDE. A classic example would be that of an administrator's workstation or an administrative console which can administer a security device (user directory, etc.), or systems upstream feeding information to connected systems (e.g. patching system, or an http connection as described above). In the case of a user directory, an administrator could potentially grant himself (or others) rights to systems in the CDE and breach the security of the CDE.

Indeed, the standard states that any system that "could impact the security of the CDE" is in scope. We can refer to these systems as connected/indirectly. The May 2017 Scoping Guidance refers to these as a "[s]ystem component indirectly connects to CDE". The OPST calls these "2x".

Fourth category: Out-of-scope systems

Finally, any system that is neither a CDE or a connected system is considered out-of-scope for PCI compliance. That system must be completely isolated (no connections whatsoever) from CDE systems, though it may interact with connected systems (and can even reside in the same network zone with connected systems). Do remember, however, if it can affect security of the CDE indirectly through another connected system, that it is a connected system and is therefore in scope.

Out-of-scope systems are generally represented in **green**. The May 2017 Guidance for PCI DSS Scoping and Network Segmentation provides four (4) tests that must be passed to confirm that a system is out-of-scope (which amount to ensuring that the system does not fall under the previously defined categories) and with my take on them following the arrow (=>):

- System component does NOT store, process, or transmit CHD/SAD => otherwise it would be a CDE/CHD system.
- System component is NOT on the same network segment or in the same subnet or VLAN as systems that store, process, or transmit CHD => otherwise it would be a CDE/contaminated system.
- System component cannot connect to or access any system in the CDE => otherwise it would be a connected/communicating system (although I still contend that some connections could be considered out-of-scope if one can demonstrate they pose no risk, such as pings).
- System component cannot gain access to the CDE nor impact a security control for CDE via an in-scope system => otherwise this is a connected/security or connected/indirectly system.

The OPST calls these category "3".

Categories Summary

To summarize, there are four basic types of systems for PCI DSS purposes. The first group is the Cardholder Data Environment (CDE). The second group is comprised of segmenting systems, which are required to enable the other groups. The third group are connected systems, those that have some direct or indirect connection into the CDE (which the May 2017 Scoping guidance calls "Connected-to or Security-impacting Systems"). The fourth are out-of-scope systems completely isolated from the CDE systems. For these, always remember that "[s]ystems that could impact the security of account data or the CDE (for example, name resolution, or e-commerce (web) redirection servers)." They are always in scope or, to put it in other words: "If it can impact the security of the CDE, it is in scope".

Classification is key for us so we don't have to apply PCI DSS requirements to all systems.

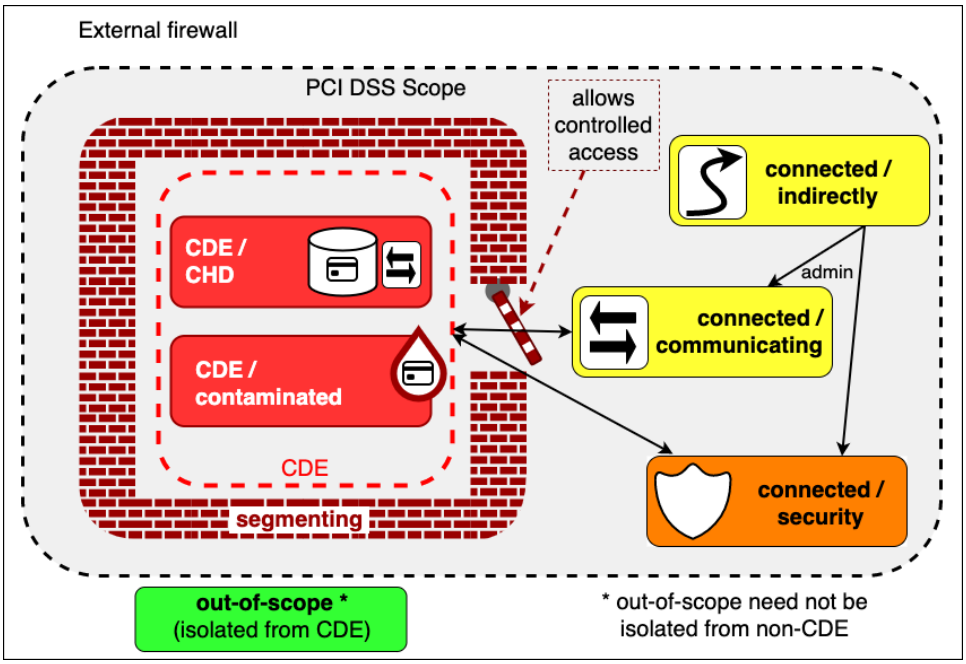

Figure 3 - PCI Resources PCI Scope Type Diagram

Type	Sub-Type	Segmentation	CHD/SAD	In-Scope
CDE	CHD	None	Yes	Yes
CDE	Contaminated	None	No	Yes
Segmenting		Provides Segmentation	No	Yes
Connected	Communicating	Controlled Access	No	Yes
Connected	Security	Controlled Access	No	Yes
Connected	Indirectly	Indirect Access	No	Yes

Type	Sub-Type	Segmentation	CHD/SAD	In-Scope
Out-of-scope		Isolation	No	No

Table 1 - PCI Resources Classification Categories Summary

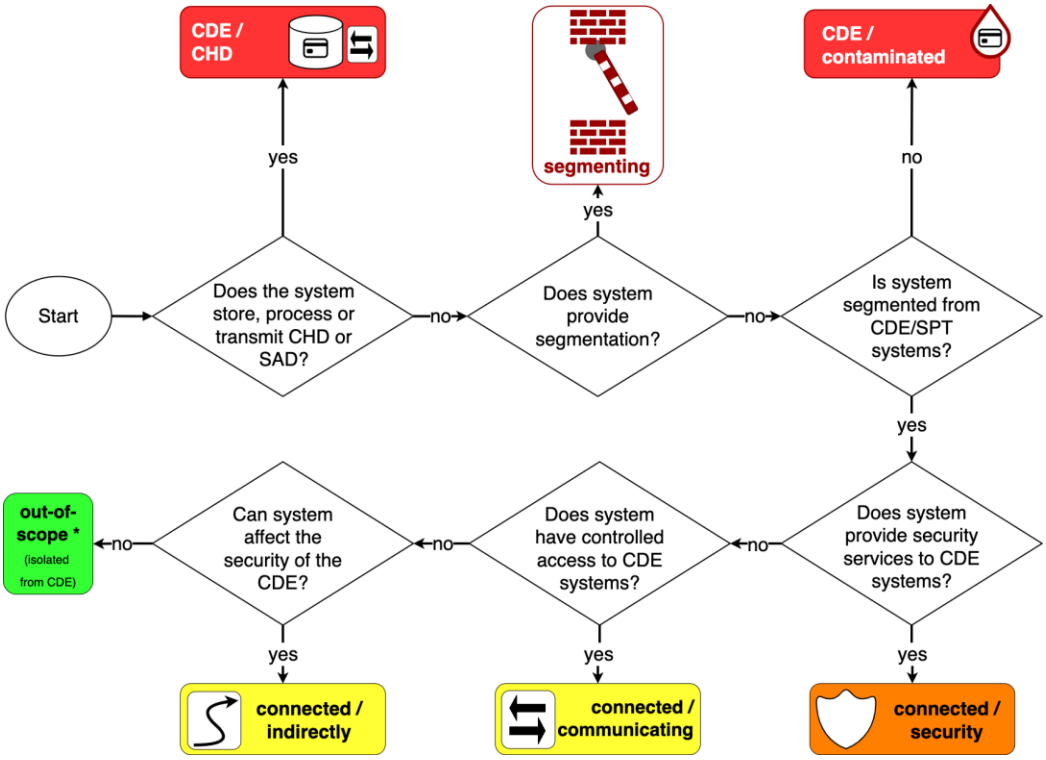

Figure 4 - PCI Resources PCI Scoping Type Decision tree

Scope Identification approach and Scope Documentation

Now that we've described the scope classification model, we need to look at how we must properly document the scope. The approach follows the model closely, with some elements of validation added. Once again, requirement 12.5.2, adapted from A3.2.1 of the 4.0 standard provides us with the overall approach, while Appendix A3 (DESV) previously added more guidance of this definition in requirements A3.2.*. As we have 2 categories (types) of in-scope systems (CDE and connected), we'll be splitting the process in two parts, one for each type.

Part 1 - Identifying the CDE (a four-step process)

Step 1.1 - Identify all systems that store, process or transmit Account Data (CHD or SAD) (CDE/CHD systems). These include servers, workstations, appliances, network equipment, etc. The flow of Account Data must be documented in diagrams (1.2.4, v3#1.1.3) and detailed textual descriptions need to be produced (RoC #4.2.1). The flows and description must cover capture, authorization, settlement, chargebacks and refunds (1.2.4, v3#1.1.3).

Step 1.2 - Identify where segmentation occurs (Segmenting systems). Segmenting systems prevent contamination and limit the scope of the CDE. The identified segmented CDE zones are generally represented in red in network diagrams.

Note: any time you implement a new type of segmentation, you should perform segmentation testing as demanded by requirement 11.4.5, v3#11.3.4 and confirm its effectiveness (and fix issues identified) before deploying the new technology into production (also called for in A3.2.4).

Step 1.3 - Identify all other systems within the CDE which are contaminated (CDE/contaminated) systems. This should use the current maintained inventory (required by 12.5.1, v3#2.4) but also include a system discovery using scanning tools (ping sweeps are typical here). Any difference with the inventory should be an indication of a failing inventory process and used to review and correct that process. The systems covered include servers, workstations, appliances, network equipment in the same segmented network zones or running under the same Segmenting hypervisors.

Note: since CDE/contaminated systems bring potential scope reduction opportunities, this step can be used to review if it makes sense to move the system outside the CDE.

Step 1.4 - Finally, validate that we do not have other PAN in other systems (12.5.2, adapted from A3.2.1) or locations which the requirement states as "[i]dentifying all locations where account data is stored, processed, and transmitted, including but not limited to:" and "1) any locations outside of the currently defined CDE". This "data discovery" is usually performed using specialized tools (Data Loss Prevention, DLP) but simple 'grep' on Unix/Linux also works. These searches generally use Regular Expressions, but manual discovery may be applicable when few systems are to be reviewed or on systems where such tools may not exist (for example, mainframes). For those who are resource constrained, inexpensive and free options do exist.

The "data discovery" should be performed on any system with the potential of storing PAN; at a minimum, this should cover all systems in the CDE and all connected systems (but really should include all servers, desktops and laptops). If any system is identified with PAN, then the following options are possible:

- Consider the system as a CDE/CHD system and perform anew the previous identification steps
- Migrate the system into the CDE and redo the previous steps
- Securely delete the CHD, and determine why and how PAN was transferred to the system or location to prevent further expansion of scope

In all cases, this should be treated as a security incident per requirement section 12.10.

Note 1: Version 4.0 of PCI DSS clarified the scope of what should be checked when it added the following line: "*All types of systems and locations should be considered during the scoping process, including backup/recovery sites and fail-over systems.*"

Note 2: This is also an appropriate time to review requirement 3.2.1, v3#3.1 and testing procedure 3.2.1.c to ensure that Account Data (CHD and SAD) is destroyed after the approved retention period.

Part 2 - Identify connected systems (a five-step process)

Once the CDE has been properly validated comes the time to identify the remaining in-scope systems.

Step 2.1 - Review all the in-scope NSC (firewall or equivalent equipment implementing the ACLs) rules of Segmenting systems to identify the list of all systems that may connect to the CDE. If the rules are for network ranges instead of individual systems, then using a system discovery tool for the entire range may be required (see step 1.3 of CDE identification). Note that if a rule implies a system that no longer exists, then that rule needs to be removed as required by 1.2.7, v3#1.1.7. The fact that a decommissioning did not remove a system from a firewall ruleset should be treated as an incident and call for a review of the change control process. With the complete list (of IP addresses or systems), we will proceed in classifying these systems according to the model.

Step 2.2 - Identify any systems which provide security services, or services that may affect the security of the CDE, and which will be classified as connected/security systems. These include, at a minimum:

- Identity and Directory Services (Active Directory, LDAP)
- Domain Name Systems (DNS), Network Time Systems (NTP)
- Patch management systems
- Vulnerability management systems
- Anti-virus management systems
- File Integrity Management or Change Detection systems
- Performance Monitoring Systems
- Encryption Key Management Systems
- Remote-access (VPN) Systems
- Multi-factor Authentication Systems
- Log Management Systems and Monitoring Solutions (SIEM, syslog, etc.)
- Intrusion Detection Systems/ Intrusion Prevention Systems (IDS/IPS)

Step 2.3 - Identify third-party systems that may be connected to the CDE through some sort of Internet or private link. These systems are out of your control; they are the responsibility of the third-party service providers (TPSP) that manage them. But you nonetheless have responsibility to include those TPSP in the in-scope provider list (12.8.1) and ensure they are adequately managed according to requirements 12.8.*. Remember that if the connections go through internal network equipment such as routers, then those will still be in scope.

Step 2.4 - Identify connected systems that only receive information and which may (through analysis) be deemed out-of-scope if they pose 'no risk' to the CDE. These systems generally cannot initiate a connection to the CDE and do not have a re-entry to the initiating system (ping or the ICMP protocol may be an exception). This could be the case of an sftp connection, as described earlier. Note that some protocols (DNS, NTP) that might have been deemed as out-of-scope have been used in previous breaches to exfiltrate information. In these cases however, IDS/IPS, DLP or other controls on the CDE connection points or on the initiating system may be more appropriate to monitor for security. The analysis should be thoroughly documented and this documentation must be maintained for review by your assessor (QSA, ISA, etc.).

The remaining systems of the list identified in the first step are simply connected/communicating systems.

Step 2.5 - Finally, identify systems that are isolated from the CDE but could still affect its security, indirectly through some other connected system. These are obviously classified as connected/indirectly. Often, these are administrative consoles or administrator desktop/laptops.

Additional Guidance

The RoC reporting template gives us more detail on what we must document. Our documentation should include the information in the following subsections of sections 2, 3, 4 of the RoC reporting template. The ones marked as "assessor" are for use by the assessor, not the entity, although the assessor could be internal, either an ISA or someone producing a Self-Assessment Questionnaire (SAQ).

Section		**Detail**
2	Business Overview	Title
2.1	Description of the Entity's Payment Card Business	
3	Description of Scope of Work and Approach Taken	Title
3.1	Assessor's Validation of Defined Scope Accuracy	Assessor
3.2	Segmentation	How segmentation is implemented
3.3	PCI SSC Validated Products and Solutions	Published on the PCI SSC website
3.4	Sampling	Assessor
4	Details About Reviewed Environments	Title
4.1	Network Diagrams	PCI DSS 1.2.3, v3#1.1.2
4.2	Account Dataflow Diagrams	PCI DSS 1.2.4, v3#1.1.3
4.3	Storage of Account Data	A subset of CDE/CHD systems
4.4	In-scope Third-Party Service Providers (TPSPs)	PCI DSS 12.8.*
4.5	In-scope Networks	All CDE zones containing systems that Store, Process, or Transmit (SPT) Account Data (CHD and SAD)
4.6	In-scope Locations/Facilities	Physical locations where in-scope systems are located
4.7	In-scope Business Functions	In-scope business processes
4.8	In-scope System Component Types	CDE and connected system types (routers, servers, etc.)
4.9	Sample Sets for Reporting	Assessor

Table 2 - RoC reporting template sections for scope documentation

The subsections marked as "Assessor" would be filled by the assessor during the compliance assessment (RoC or SAQ). The ones marked as "Title" are simply headers.

References:

This model draws on pages 9 through 18 of the PCI DSS 4.0 standard and on a few other documents, listed here:

- A presentation by the PCI SSC at the RSA conference in 2013 [1] (public) and a similar slides deck from the 2013 PCI community meetings (available to PCI assessors: QSAs, ISAs, PCIPs)
- PCI SSC answers to Frequently Asked Questions (FAQ) [2]
- PCI DSS Designated Entities Supplemental Validation for 3.1 (DESV, released June 2015) - A new set of requirements to increase assurance that an organization maintains compliance with PCI DSS over time, and that non-compliance is detected by a continuous (if not automated) audit process; this set of requirements applies to entities designated by the card brands or acquirers that are at a high risk level for the industry. DESV is now integrated as Appendix A3 in PCI DSS 4.0. [3]
- RoC reporting template for PCI DSS 4.0 [4]
- Information Supplements:
    - Best Practices for Maintaining PCI DSS Compliance (released August 2014 but updated March 2016 and again in 2019) [5]
    - Protecting Telephone-based Payment Card Data v.3.0 (March 2011, updated November 2018) [6]
    - Third-Party Security Assurance [7] (released August 2014 but updated March 2016)
    - PCI DSS Cloud Computing Guidelines (February 2013, updated April 2018) [8]
    - PCI DSS Virtualization Guidelines v2.0 [9] (June 2011)
    - Guidance for PCI DSS Scoping and Network Segmentation (v1.0 December 2016, updated to v1.1 in May 2017) [10] (this supplement will be referred to as the "May 2017 Scoping Guidance"); it is partly integrated in PCI DSS 4.0 which refers to it for more details

[1] PCI Security Standards Council (2013). RSA Conference - Less is more PCI DSS Scoping demystified. Retrieved July 2, 2015, from https://www.rsaconference.com/writable/presentations/file_upload/dsp-w21.pdf.

[2] PCI Security Standards Council (2012). FAQs. Retrieved July 2, 2015, from https://www.pcisecuritystandards.org/faq/.

[3] PCI Security Standards Council (2022). Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures - Version 4.0. Retrieved March 31, 2022, from https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf.

[4] PCI Security Standards Council (2022). ROC Reporting Template for v4.0. (PCI SSC FAQs). Retrieved July 1, 2022, from https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Reporting%20Template%20or%20Form/PCI-DSS-v4_0-ROC-Template.pdf.

[5] PCI Security Standards Council (2019). Best Practices for Maintaining PCI DSS Compliance v2.0. Retrieved July 1, 2022, from https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf.

[6] Protecting Telephone-based Payment Card Data v3.0. Retrieved July 1, 2022, from https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf.

[7] PCI Security Standards Council (2016). Information Supplement: Third-Party Security Assurance. Retrieved July 2, 2016, from https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.

[8] PCI Security Standards Council (2018). PCI DSS Cloud Computing Guidelines v3.0. Retrieved July 1, 2018, from https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

[9] PCI Security Standards Council (2011). PCI DSS Virtualization Guidelines. Retrieved July 13, 2015, from https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

[10] PCI Security Standards Council (2017). Guidance for PCI DSS Scoping and Network Segmentation. Retrieved July 1, 2018, from https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf.

Version History

Version	Author	Description	Date
1.0	Yves Desharnais	Initial release	July 2015
1.1	Yves Desharnais	Clarifications, Formatting and Update to PCI DSS 3.2 and other PCI SSC updated documents	July 2016
1.2	Yves Desharnais	Clarifications and changes related to PCI DSS Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation	December 2017
1.2.1	Yves Desharnais	Minor fixes for PCI DSS 3.2.1 and initial Spanish and French Versions	July 2018
1.3	Yves Desharnais	Update for PCI DSS 4.0	August 2022

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

You are free to:

Share — copy and redistribute the material in any medium or format
Adapt — remix, transform, and build upon the material for any purpose, even commercially.
The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the **same license** as the original.

No additional restrictions — You may not apply legal terms or **technological measures** that legally restrict others from doing anything the license permits.

Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable **exception or limitation**.

No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as **publicity, privacy, or moral rights** may limit how you use the material.

Author:
Yves Desharnais, 8850895 CANADA INC.
Email: info@pciresources.com
Website: www.pciresources.com