PCI Resources - 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. 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 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). Terms and acronyms are described towards the end of this document.

1 - PCI Resources Simplified PCI DSS Scoping Model and Approach

With the 2026 release of the book and model, I've decided to focus on the simplified approach. The details of the approach were updated to align with the simplified approach, made cleaner and more streamlined.

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, and updated in 2026 for 4.0.1 to simplify and streamline it.

While the details of the model and approach are important, they are a bit long for everyday use. For that reason, I created a simplified version with just 6 steps aligned with the categories in the model that summarizes it further.

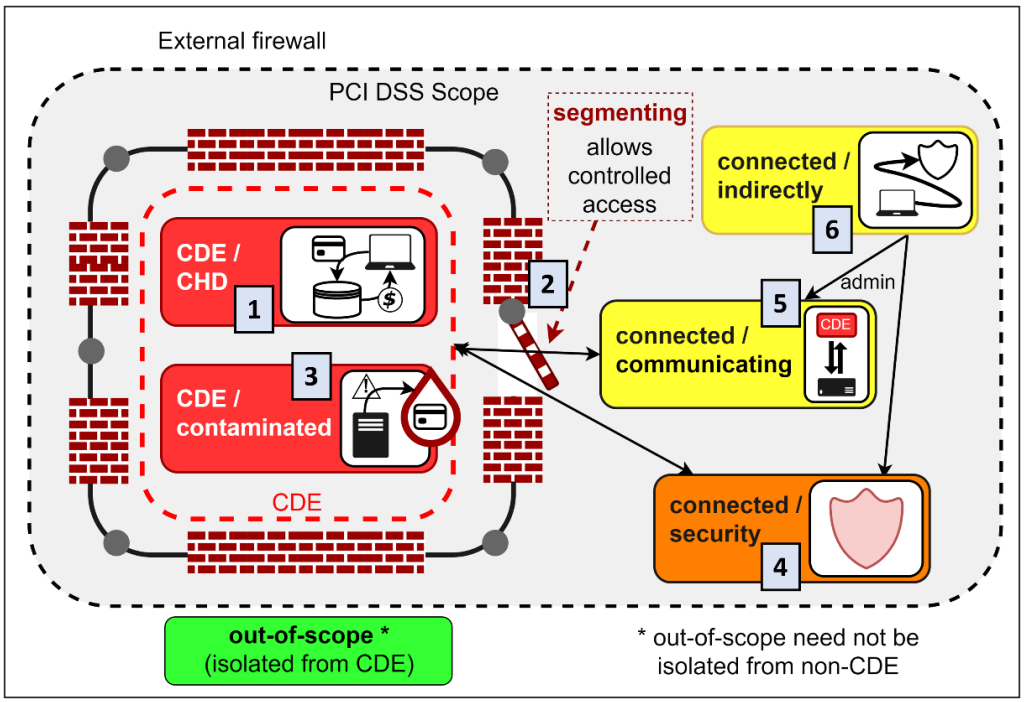


Figure 2 - PCI Resources Simplified Scoping Model

The six steps which line up with the categories require us to identify:

1. Systems that Store, Process, or Transmit (SPT) card data (CDE/CHD on the diagram)
2. Segmentation which limits scope (segmenting)
3. Systems located in the same segmented zones (CDE/contaminated)
4. Systems which either (connected/security):
   - Support PCI DSS requirements
   - Provide security services
   - Could impact the config or security of the CDE (via #1, 2, and 3)
5. Systems with a connection to anything in the CDE (connected/communicating)
6. Systems which could, indirectly, through other previously identified connected systems (connected/*) affect the security of the CDE (connected/indirectly)

* Only if a system cannot be classified in these steps can it be ruled as out-of-scope

Details of those steps are presented in the next sections.

The following decision diagram (figure 7) has outlined this approach since the first release of the model in 2015.

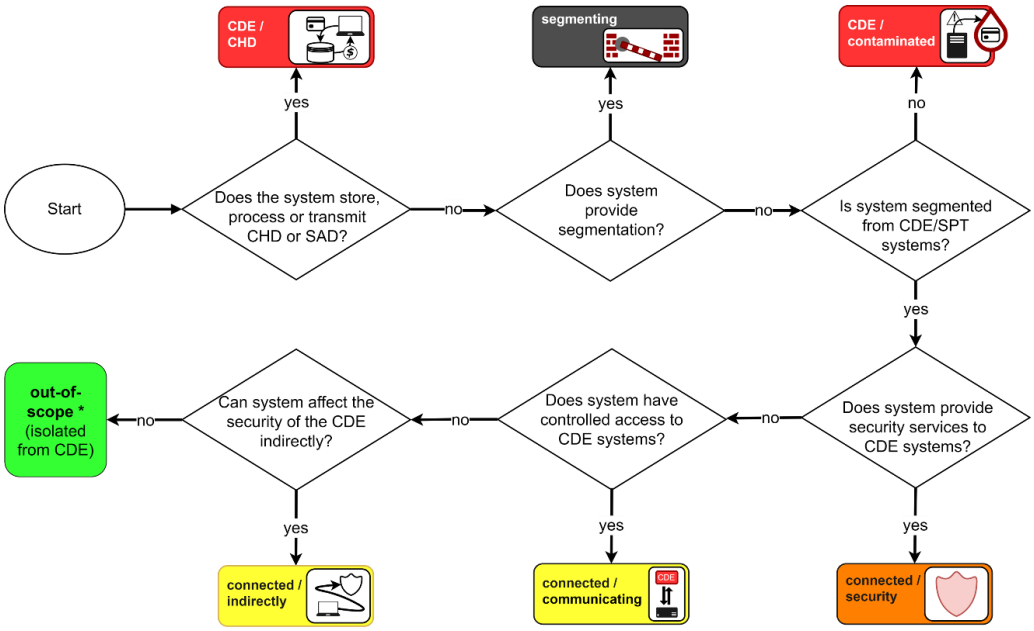


Figure 3 - PCI Scoping Type Decision tree

1.1 - Categories Summary

There are four high-level categories 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)."*[12] 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.*"[13].

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

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
Out-of-scope		Isolation	No	No

Table 1 - Classification Categories Summary

2 - Simplified Approach and 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". [14]

As a reminder, PCI DSS only defines two types of in-scope systems: CDE (cardholder data environment) and connected (connected are only possible in the presence of effective segmentation). I add segmentation since in its absence, everything is CDE. Everything else is out-of-scope for PCI DSS.

The scope definition of PCI DSS 4.0.1 is:

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.*
- *AND*
  - *System components, people, and processes that could impact the security of cardholder data and/or sensitive authentication data.*

Validation

PCI DSS 4.0 added requirement 12.5.2 that covers validation:

- *12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:*
  - *Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).*
  - *Updating all data-flow diagrams per Requirement 1.2.4.*
  - *Identifying all locations where account data is stored, processed, and transmitted, including but not limited to:*
    1. *any locations outside of the currently defined CDE,*
    2. *applications that process CHD,*
    3. *transmissions between systems and networks, and*

4. *file backups.*
   - *Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.*
   - *Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.*
   - *Identifying all connections from third-party entities with access to the CDE.*
   - *Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.*

2.1 - Simplified Approach Part 1 - CDE (steps 1-3)

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. Generally, CDE systems are generally represented in **red** (as in "danger").

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 version. 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.*

2.1.1 Step 1 - Systems that Store, Process, or Transmit (SPT) card data

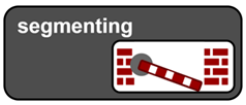
The first sub- bullet is our first category:

> *System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data,*

All these systems that SPT CHD/SAD are part of, 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 (see table 2 for a summary). The May 2017 Scoping Guidance refers to these as "[s]ystem component stores, processes, or transmits CHD/SAD". The OPST calls these "1a".

These include servers, workstations, appliances, network equipment, etc. The flow of Account Data must be documented in diagrams (1.2.4) 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).

2.1.2 Step 2 - Segmentation which limits scope (segmenting)



The latter part of the second sub-bullet states - *have unrestricted connectivity to system components that store, process, or transmit CHD/SAD* -, implicitly identifying systems that prevent contamination and limit the scope of the CDE.

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 since PCI DSS 4.0). These devices are called Segmenting systems (segmentation and its role in scope reduction will be addressed separately).

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 prevent any confusion. This is my only major disagreement with the PCI SSC document.

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.

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 demanding annual segmentation penetration testing (every 6 months for service providers with 11.4.6). The segmentation section of the scope definition includes an instruction to that effect: "If 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." [15]

2.1.3 Step 3 - Systems located in the same segmented zones(CDE/contaminated)

Getting back to 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.*

Indeed, in the 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*"[16]. Therefore, (network) segmentation - is not required other than at the external perimeter of the network (whereby its absence would be like leaving your front door wide open, or at least unlocked). The standard also adds that "[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.

Identification should use the current maintained inventory (required by 12.5.1) 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.

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 airborne virus analogy works well to explain this concept of "contamination". People contaminated with the virus are akin to systems with CHD/SAD. A person in the same room with someone that has the virus runs the risk of becoming infected themselves. The May 2017 Scoping Guidance refers to these as a "[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".

2.1.4 Validation nothing else outside CDE

Finally, validate that we do not have other PAN in other systems or locations which the requirement 12.5.2 refers to as:

[i] dentifying all locations where account data is stored, processed, and transmitted, including but not limited to:

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 and testing procedure 3.2.1.c to ensure that Account Data (CHD and SAD) is destroyed after the approved retention period.

2.2 - Simplified Approach Part 2 - Connected systems (steps 4-6)

Once the CDE and segmentation have been properly validated comes the time to identify the remaining (connected) in-scope systems.

After the CDE scope definition (first bullet and its two sub-bullets) of PCI DSS 4.0.1, 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 previously 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 and 1.3.2. 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 [17] 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*"[18]. This was 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 scope
Remember non-CHD systems may be in scope too [19]

and

If an "out-of-scope" system could lead a CDE compromise, it should not have been considered out of scope [20]

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.

Getting back to our physical analogy, anybody that can talk to someone in the room could potentially gain access to the CHD information stored on those papers either by getting their hands on it or from someone who has access to that information. Most people worry about theft (or hackers), but the "people" element (in the previously mentioned "people, processes and technologies") is often the weakest link in security. Many of the breaches involve what is called social engineering, or pretexting, which just means convincing someone to give us information (sometimes even system usernames and passwords) or performing actions on our behalf. Phishing (phony emails, the terms comes from "phone" and "fishing", basically fishing for a vulnerable user, often through phone calls) also falls within that category. I won't delve into the details of these types of attacks. Systems that are segmented but not completely isolated from the CDE systems and can communicate with CDE systems without accessing any CHD or SAD through some level of access control become "connected" systems.

In this book, we use the term 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 [21]:

- *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 (per the OPST). As in the CDE case, there are different types of "connected" devices that present a different level of risk. Let's examine those three subtypes.

2.2.1 Step 4 - Systems that can affect security of the CDE (connected/security):

There are systems which provide security services, or services that may affect the security of the CDE. These include 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'. In our physical analogies, these would be security guards which can issue keys for the room, or it could be cleaning staff that provide services for that room. We can call these connected/security systems. It should not be hard to realize why these are in scope. After all, in the real world, if you could take over the guard station, then you could theoretically walk-in to whatever area they are protecting. These could have direct connection to the CDE server or not. For example, it may be hard to consider only one server in scope for a given service. Active Directory is one of where a breach of one of its servers (even a read-only one) may leave the entire AD infrastructure compromised.

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

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 11 of the PCI DSS 4.0.1 standard.

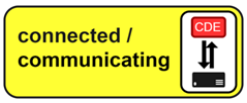
The OPST calls these "2a". A list of probable candidates include:

Sections	Category/Devices/Tools	Layer
1.2-1.4	Network Security Controls (NSC)	net
1.5	Mobile Devices (PCs, phones)	os /net
2.3,11.2	Wireless Access Points (WAP)	net
3.2-3.5	Storage (databases, file systems)	os /data
3.6-3.7	Management of Encryption Keys	os /data
4.2	Messaging and Certifications for transmission	app/ os
5.2-5.3	Antimalware	os
5.4	Anti-phishing	os /net
6.2	Software Development Security	app
6.3	Vulnerability Management, Patching,	app/ os
6.4	External web server	app/ os /net
6.5	Change Management	

Sections	Category/Devices/Tools	Layer
7.2-7.3	System access and Role-based access Controls	app/ os
8.2-8.3	User Accounts	user
8.4-8.5	Multifactor authentication (MFA)	user
8.6	System Accounts (e.g. AD, LDAP)	app/ os
9.2	Cameras & Locks/Physical Access	physical
9.4	Media management (backups)	physical
9.5	Physical Payment Devices (POI)	physical
10.2-10.3	Logging	app/ os /net
10.4-10.5	Monitoring (SIEM)	app/ os /net
10.6	Timeservers (NTP)	os
11.3	Vulnerability scanners (and/or ASV)	app/ os /net
11.5.1	IDS/IPS	net
11.5.2	Change Detection / FIM	app/ os
11.6	Monitoring payment pages	app/ os /net
12.5	Inventory management system (e.g. CMDB)	
12.6	Security Awareness	user
12.8	Third-Party management	
12.10	Incident Responses	

Table 2 - PCI DSS 4.0.1 sections and possible list of in-scope device types

2.2.2 Step 5 - Systems with a connection to anything in the CDE (connected/communicating)



In addition to security services, 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.

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.

To ensure completeness, I would recommend that you 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 3 for contaminated systems of the CDE). Note that if a rule implies a system that no longer exists, then that rule needs to be removed as required by requirement 1.2.7. 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.

We must also 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 likely be in scope.

Finally, we should 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.).

2.2.3 Step 6 - Systems which could, indirectly, through other previously identified connected systems (connected/*) affect the security of the CDE (connected/indirectly)

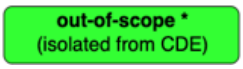
There are also systems that do not have any direct access to CDE systems (they are isolated from the CDE) but that are still in scope. Instead, they would generally have access to other connected or segmenting systems and, through these, could affect the security of the CDE. A classic example would be 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. The use of some non-deterministic systems outside the CDE such as genAI/LLM could also potentially fall here depending on their implementation in the environment.

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".

In our continued analogy, indirectly connected could mean a supply company, such as a food ordering service that, if compromised, could provide with nefarious intent drugged food to the staff or security personnel.

2.3 - Out-of-scope systems



Finally, any system that is neither a CDE, segmenting, 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.

The May 2017 Scoping 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".

2.4 - Scope Documentation

While there is no formal template or guidance on what and how to document scope, I've documented what is required leveraging both the requirements and reporting templates; this guidance is presented in Appendix 2A also made available for free on the book companion website.

3.1 - Terminology and 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.

A glossary is provided at the end of the book and on the companion website.

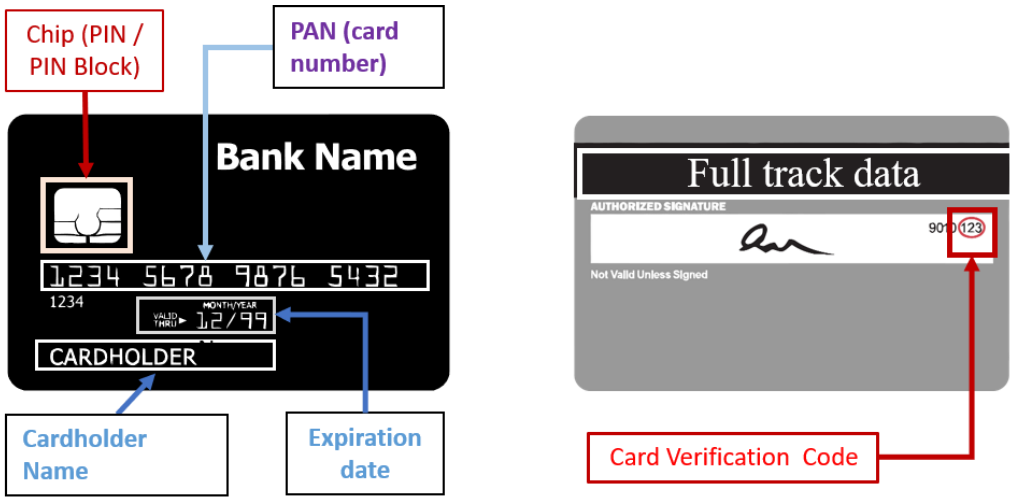


Figure 1 - Rendering of Payment Card (Front and Back) with data elements

3.2 - References

This model draws on pages 9 through 18 of the PCI DSS 4.0.1 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.

3.3 - 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
2.0	Yves Desharnais	Update for PCI DSS 4.0.1 and the simplified approach	August 2026

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