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 December 2016 PCI DSS Information Supplement from the PCI SSC and called "Guidance for PCI DSS Scoping and Network Segmentation" (this supplement will be referred to as the "December 2016 Guidance". No substantive changes were made, only clarifications added.

Acronyms

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

- CHD = Acronym for "Cardholder Data"; consists of the PAN, cardholder name, card expiration date, and sometimes service code
- PAN = Acronym for "Primary Account Number"; the card number printed on the front of the card.
- SAD = Acronym for "Sensitive Authentication Data", it includes the magnetic track information, the PIN or PIN block, as well as the Card-not-present authorization value which we'll refer to as CVV2 but can take any of the following acronyms: 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 CHD or SAD but is not limited to these.
- Isolation = There is no possible access between systems.
- Controlled Access = There are limited (restricted) communications possible between systems.
- RoC = Report on Compliance
- Entity = An entity is any organization that has the responsibility to protect card data; for PCI DSS compliance, an entity will be defined as either a merchant or a service provider.
- DESV = PCI DSS Designated Entities Supplemental Validation for PCI DSS 3.1, a new PCI standard released in June 2015 which is now integrated as appendix A3 of PCI DSS 3.2
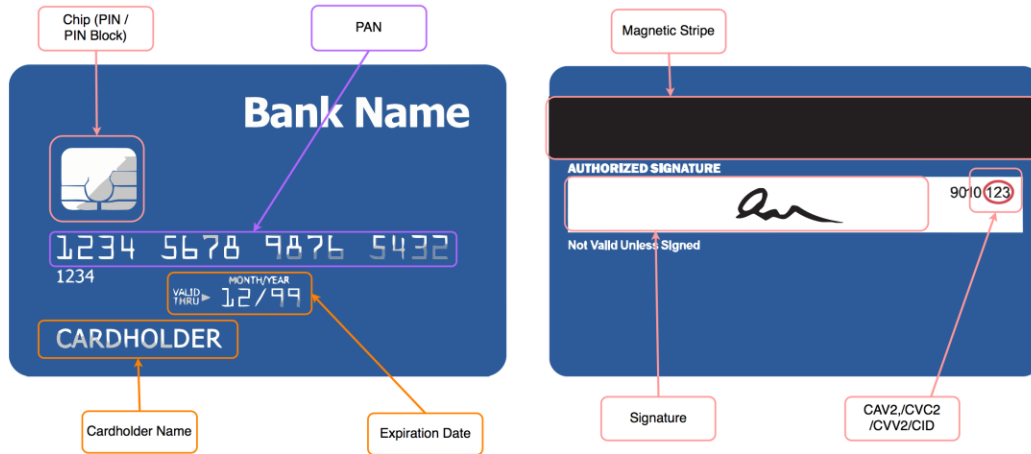
Figure 1 - Rendering of Credit Card (Front and Back) showing CHD and SAD

Scoping categories

My approach to scoping, 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 both 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.

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?*" starting 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 all each of the requirements. Generally, CDE systems are represented in ***red***.

CDE/CHD

The Scope of PCI DSS is presented on page 10 of version 3.2 of the standard. The first paragraph states:

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

Let's break this paragraph into its important aspects.

- "*apply to all **system components**" - adding that they "*include network devices, servers, computing devices, and applications.* " - so basically, any type of computer system (hardware, operating system, software, applications) is subject to the requirements.

- "*(CDE) is comprised of people, processes and technologies*" - so, while PCI DSS applies to computer systems, people and processes are also critical (and I recommend, as many others do, taking a business process approach first).
- "*that store, process, or transmit cardholder data or sensitive authentication data*" - what will often refer to as SPT CHD/SAD to summarize. The systems that come into contact with CHD or SAD are the main ones we are trying to protect since they hold, or have access to, the information (the goods) that we are required to protect.

All these systems that SPT CHD/SAD are part, or form the basis, of your CDE (Cardholder Data Environment - the environment in scope for PCI). We'll refer to these as CDE/CHD systems. The December 2016 Guidance refers to these as "[s]ystem component stores, processes, or transmits CHD/SAD". The OPST calls these type "1a".

CDE/Contaminated

In the network segmentation section, the standard states that *"[n]etwork segmentation of, or isolating (segmenting), the cardholder data environment 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 network segmentation (sometimes called a 'flat network') the entire network is in scope of 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 December 2016 Guidance calls these systems *"System 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"*.

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. Typically, these are firewall devices, but they are not limited to those. These devices are called Segmenting systems. The scope definition includes an instruction to that effect (present in previous PCI DSS versions): "If network segmentation is in place and being 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."

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. Thus, what the PCI SSC December 2016 Guidance calls "System component segments CDE systems from out-of-scope systems and networks", but puts in the connected systems category ("Connected-to or Security-impacting Systems") I will mark at its separate category to prevent any confusion (it is my only disagreement with the PCI SSC document, but this difference is more stylistic than anything else).

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 (#11.3.4).

Section 3.3 (Network Segmentation) of the PCI DSS 3.2 RoC template adds documentation of this validation of adequate segmentation was performed. Note that the 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.
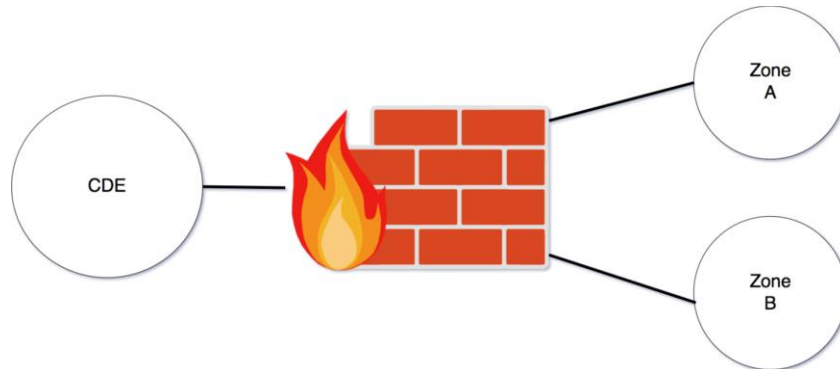

Figure 2 - Image of firewall and 3 network zones (including the CDE)

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

Ultimately, unless using a straightforward segmentation device such as a physical firewall, entities you should provide an evaluation that covers requirement 11.3.4 demanding network segmentation penetration testing.

Segmenting systems are generally represented in orange.

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.

For more detail see section 2.7 of Volume 2.

Third category: Connected systems

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 the systems must be restricted to only those services required for business operations (called "controlled access") according to requirement #1.2.1. 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 standard states that any device that is "connected to the cardholder data environment" (CDE) is in scope since it is not completely isolated. The standard includes in scope any "[s]ystems that 'may impact the security of' (for example, name resolution or web redirection servers) the CDE". This is likely one of the most important lines written on scoping in the standard. 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 scope*
> *Remember 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 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'. 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.

The December 2016 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 welcomed.

The OPST calls these "2a".

Connected/Communicating Systems

Any system that is 'connected to' the CDE (to CDE systems) is considered a 'connected' system. The exception is systems that are 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 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 of 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 insured 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). Documentation of the evaluation process should be created, maintained and kept, to be presented to your assessor. The December 2016 Guidance calls these systems "System component directly connects to CDE". The OPST calls these "2b" or "2c"; I don't make the distinction based on flow-direction, but on details of communication.

Connected/Indirectly

There are also systems that do not have any direct access to CDE systems (they are isolated from the CDE) 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 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 "may impact the security of the CDE" is in scope. We can refer to these systems as connected/indirectly. The December 2016 Guidance calls these systems "System 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 December 2016 Guidance for PCI DSS Scoping and Network Segmentation provides 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):

- 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 segmenting systems, which are required to enable the other groups. The third group are connected systems, those systems that have some direct or indirect connection into the CDE (which the December 2016 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 may impact the security of (for example, name resolution or web redirection servers) the CDE" 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.
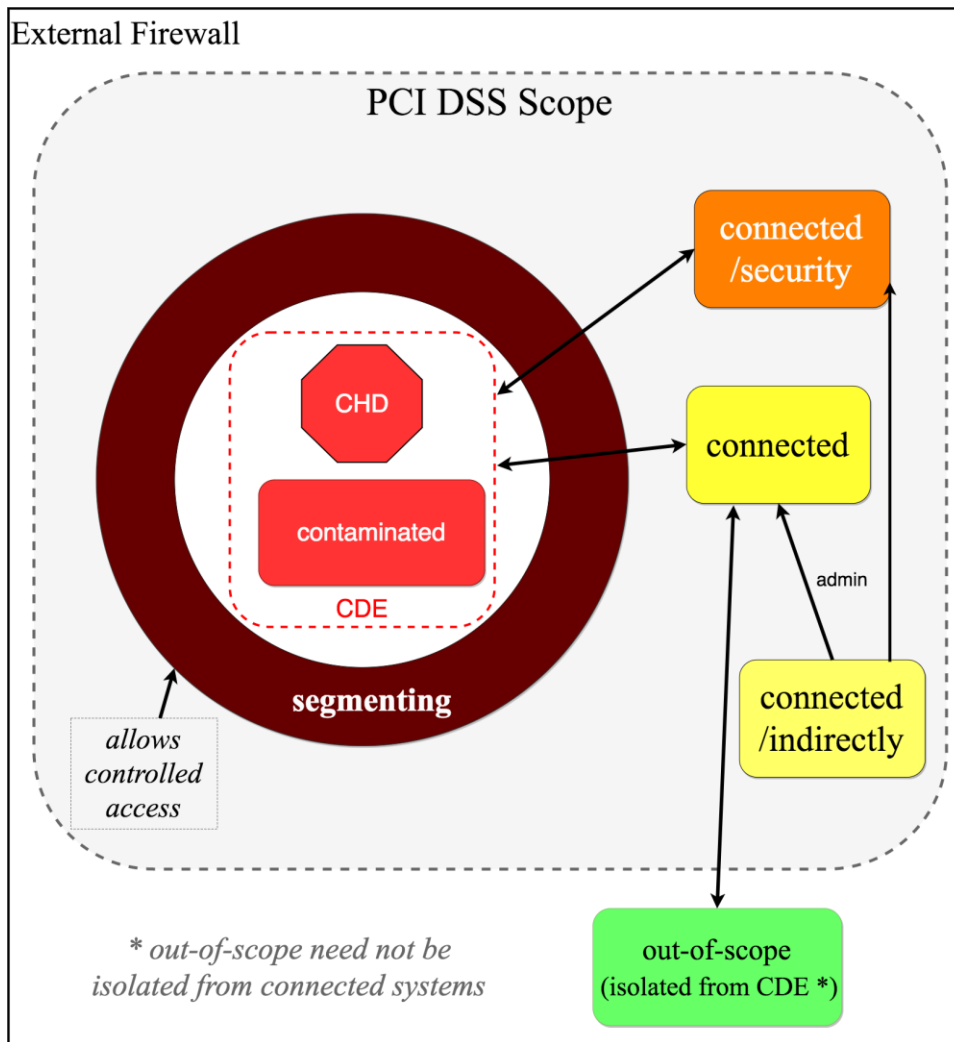
Figure 3 - PCI Scope Type Diagram

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
Out-of-scope		Isolation	No	No

Table 1 - Classification Categories Summary
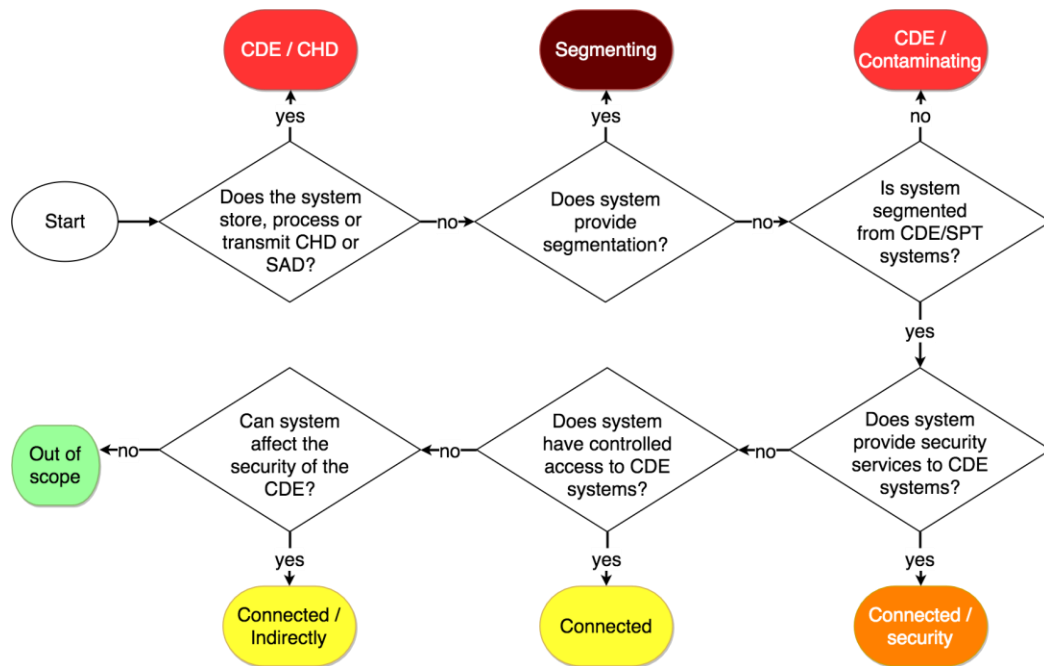
Figure 4 - PCI Scoping Type Decision tree

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, pages 10 and 11 of the standard provide us with the overall approach, while Appendix A3 (DESV) added more guidance of this definition in requirements A3.2.* (DE.2.* in DESV). As we have 2 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 CHD/SAD (CDE/CHD systems). These include servers, workstations, appliances, network equipment. The flow of CHD must be documented in diagrams (#1.1.3) and detailed textual descriptions need to be produced (RoC #4.2). The flows and description must cover capture, authorization, settlement and chargebacks.

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 #11.3.4 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 #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 (more on hypervisors in section 2.7.1 on virtualization).

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. More on this in volume 3 on TCO (Total Cost of Ownership).

Step 1.4 - Finally, validate that we do not have other PAN in other systems (#A3.2.5) or locations. 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 #12.10.*.

Note 1: Version 3.2 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 as part of the scoping process, including backup/recovery sites and fail-over systems.* "

Note 2: This is also an appropriate time to review requirement #3.1 and testing procedure #3.1.b to ensure that CHD 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 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 will 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 #1.1.7. 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, 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 which are out of your control are also out-of-scope, but the third-party providers must be managed as stated by requirements #12.8.*. Remember that if the connections go through internal network equipment such as routers, then that equipment 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 of 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	Summary Overview	Title
2.1	Description of the entity's payment card business	
2.2	High-level network diagram(s)	PCI DSS 1.1.2
3	Description of Scope of Work and Approach Taken	Title
3.1	Assessor's validation of defined cardholder data environment and scope accuracy	Assessor
3.2	Cardholder Data Environment (CDE) overview	People, Process, Technology
3.3	Network segmentation	How segmentation is implemented
3.4	Network segment details	All CDE zones containing systems that SPT CHD/SAD
3.5	Connected entities for processing	PCI DSS 12.8.*
3.6	Other business entities that require compliance with the PCI DSS	
3.7	Wireless summary	
3.8	Wireless details	
4	Details about Reviewed Environment	Title
4.1	Detailed network diagram(s)	PCI DSS 1.1.2
4.2	Description of cardholder data flows	PCI DSS 1.1.3
4.3	Cardholder data storage	A subset of CDE/CHD systems
4.4	Critical hardware in use in the cardholder data environment	CDE systems and connected/security
4.5	Critical software in use in the cardholder data environment	CDE systems and connected/security
4.6	Sampling	Assessor
4.7	Sample sets for reporting	Assessor
4.8	Service providers and other third parties with which the entity shares cardholder data	PCI DSS 12.8.*
4.9	Third-party payment applications/solutions	PA-DSS
4.1	Documentation reviewed	Assessor
4.11	Individuals interviewed	Assessor
4.12	Managed service providers	Included in-scope or PCI DSS 12.8.*
4.13	Disclosure summary for "In Place with Compensating Control" responses	Assessor
4.14	Disclosure summary for "Not Tested" responses	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 10 and 11 of the standard and on a few other documents:

- 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 PCI DSS 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 3.2. [3]
- RoC reporting template [4]
- Information Supplements:
    - Best Practices for Maintaining PCI DSS Compliance (released August 2014 but updated March 2016) [5] (which is in many ways superseded by DESV)
    - Protecting Telephone-based Payment Card Data (March 2011) [6]
    - Third-Party Security Assurance [7] (August 2014)
    - PCI DSS 2.0 Cloud Computing Guidelines [8] (February 2013)
    - PCI DSS Virtualization Guidelines v2.0 [9] (June 2011)
    - PCI DSS Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation [10] (December 2016)

[1] (RSA PCI DSS Scope, 2013). less is more pci dss scoping demystified - RSA Conference. Retrieved July 2, 2015, from https://www.rsaconference.com/writable/presentations/file_upload/dsp-w21.pdf.

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

[3] PCI DSS 3.2.1. Retrieved July 1, 2018, from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

[4] RoC reporting template. (PCI SSC FAQs). Retrieved July 1, 2018, from https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-ROC-Reporting-Template.pdf.

[5] (2014). Best Practices for Maintaining PCI DSS Compliance. Retrieved July 2, 2015, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf.

[6] (2011). Protecting Telephone-based Payment Card Data - PCI ... Retrieved July 2, 2015, from https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf.

[7] (2016). Third-Party Security Assurance v1.1 - PCI Security Standards. Retrieved May 31, 2016, from https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.

[8] (2013). PCI DSS Cloud Computing Guidelines - PCI Security ... Retrieved July 13, 2015, from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf.

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

[10] (2017). December 2016 PCI council scoping guidance vs PCI Resources model - PCI Resources. Retrieved January16, 2017, from https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.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

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