This appendix is excerpted verbatim from Volume 2 (PCI DSS Scoping) of the PCI Resources book series covering the PCI DSS (the physical book is called PCI DSS made easy). It is provided in hopes it helps the community understand what scope documentation requires.

Appendix 2A - PCI DSS Scope Documentation Guidance for PCI DSS 4.0.1

2A.1 PCI DSS Scope Documentation Guidance

2A.1.1 Preamble

Proper documenting of PCI DSS scope is often referred to as requirement 0 of PCI DSS. PCI DSS 4.0 finally added a section (12.5) dedicated to it, including a specific new requirement (12.5.2, adapted from A3.2.1) to validate scope. Hopefully this helps address the lack of understanding that led to the PCI Resources PCI DSS scoping model and approach; it was initially made available to all for free in July 2015, and further updated multiple times since based on guidance provided to all by the PCI council (PCI SSC) released. I'll reference that model in this guidance document. You can find the latest version here: http://www.pciresources.com / pci - dss -scoping-model-and-approach/ (also available there in a convenient PDF format).

Ultimately proper scope definition means that an assessor must be able to understand how PCI account data (and other relevant data flows such as authentication) flows from people (customers and users) using devices and applications, running on systems and communicating over the different network segments located in different physical locations. The required descriptions and diagrams must meet this intent.

Scope is also required to confirm an accurate inventory of system components (12.5.1) and relevant third-party service providers (12.8.1) so we can ensure all requirements are met for all components (at the network, system and application levels) and that may be shared among groups and organizations. This will also ensure testing covers all elements, whether through penetration testing (section 11.4.*) and network segmentation penetration testing (11.4.5), vulnerability scans (11.3.*), etc.

2A.1.2 PCI DSS Requirements

PCI DSS 4.0.1 includes multiple requirements that form part of scope documentation, mostly for inventories and diagrams.

PCI DSS 4.0.1 has 2 requirements, 1.2.3 and 1.2.4, that call for diagrams to be produced by the entity. These are covered in section 2A.2.

PCI DSS 4.0 added a section (12.5) covering scope. Its first requirement is the system component inventory requirement (12.5.1), followed by requirement 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. [i]

Requirement 12.5.2.1 only increases the frequency from annual to every 6 months for the validation of scope in case the entity is a service provider.

Multiple other requirements cover inventories (some are a subset of 12.5.1), including:

- System Level
    - In-scope System Component Types (categories of 12.5.1) - used for hardening (2.2.*), validation of end-of-support / EOL (12.3.4)
    - Systems without Antimalware (5.2.3)
    - Wireless Access Points (WAP) (11.2.2)
- Application Level
    - Software Dependencies (6.3.2) also often called Software Bills of Materials (SBOM)
- Data Level
    - Data Inventories (3.2.1)
- Network Level
    - List of NSC Rules / Access Control Lists (ACLs) (1.2.5)
    - List of certificates used for transmission of CHD (4.2.1.1)
- Physical Level
    - List of Physical Locations & Rooms (9.2.*)
    - List Media & physical backup sites (9.4.*)
    - List Point-of-interaction (POI) i.e. Payment Devices (POS, ATM) (9.5.1.1)

We also have the list of In-scope Third-Party Service Providers (TPSPs) (12.8.1).

2A.1.3 PCI DSS Report Sections

The different reports that entities must produce gives us more detail on what we must document. We'll look at 3 **reports** here. The Report on Compliance (RoC) reporting template is the most detailed, while the SAQ-D SP, SAQ-D M have less documentation requirements. We're presenting the RoC as the base and referencing relevant sections by location in the 2 SAQ where applicable.

Our documentation should include the information in the following subsections of sections 2 to 5 of the RoC reporting template.

ROC		SP	M	Reference
2	Business Overview			Title (no content)
2.1	Description of the Entity's Payment Card Business	Part 2A / 2c	Part 2A / 2c	PCI DSS 12.5.2 (step 1)
3	Description of Scope of Work and Approach Taken	-	-	PCI DSS 12.5.2
3.1	Assessor's Validation of Defined Scope Accuracy	-	-	Not scope
3.2	Segmentation			Segmenting systems (step 2)
3.3	PCI SSC Validated Products and Solutions	Part 2e	Part 2e	Potentially part of 12.8.1
3.4	Sampling	-	-	Not scope
4	Details About Reviewed Environments	Section 2a	-	Title (no content)
4.1	Network Diagrams	Section 2a	-	PCI DSS 1.2.3
4.2	Account Dataflow Diagrams	-	-	PCI DSS 1.2.4
4.3	Storage of Account Data	Section 2a	-	A subset of CDE/CHD systems
4.4	In-scope Third-Party Service Providers (TPSPs)	Part 2f	Part 2f	PCI DSS 12.8.1
4.5	In-scope Networks	-	-	All CDE zones containing systems that SPT CHD/SAD
4.6	In-scope Locations/Facilities	Part 2d	Part 2d	Physical locations - PCI DSS 9.2.*
4.7	In-scope Business Functions	-	-	CDE and connected business and IT processes
4.8	In-scope System Component Types	Section 2a	-	CDE and connected systems

ROC		SP	M	Reference
4.9	Sample Sets for Reporting	-	-	Not scope
5	Quarterly Scan Results	Section 2a	-	PCI DSS 11.3.*
5.1	Quarterly External Scan Results	Section 2a	-	PCI DSS 11.3.2
5.2	Attestations of Scan Compliance	Section 2a	-	
5.3	Quarterly Internal Scan Results	-	-	PCI DSS 11.3.1

Appendix 2A - Table 1 - PCI DSS 4.0.1 report template sections for scope documentation

The subsections marked as "Not scope" are not scope related but refer to the assessment itself and would be filled by the assessor during the compliance assessment (RoC or SAQ).

2A.1.4 PCI DSS Devices from Requirements

Some types of in-scope devices (both CDE and connected systems) and categories of systems can be derived from the requirements. This list is to inform and validate scope since different entities can implement things in different ways.

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	
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

Sections	Category/Devices/Tools	Layer
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	

Appendix 2A - Table 2 - PCI DSS 4.0.1 sections and possible list of devices

2A.2 PCI DSS Scope Diagram Guidance Introduction

Many firms produce PCI DSS diagram guidance internally for their assessors, and sometimes for their clients, but treat it as trade secrets and do not share it openly. I've seen a few versions of these throughout the years. I believe that providing open guidance will help the industry improve its security. It is my hope that feedback received from the community will improve this guidance over time. This guidance is what I use for my work and share with my clients.

2A.2.1 Preamble

PCI DSS 4.0.1 has 2 requirements, 1.2.3 and 1.2.4, that call for diagrams to be produced by the entity (for PCI DSS, 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). These diagrams can be created by the entity (internally) or the assessor could do it for them. The important thing is that they are created and maintained.

2A.2.2 Scope diagram requirements

The PCI DSS standard includes the two (2) previously mentioned requirements for diagrams (testing procedures are omitted here) [ii] [1].

	PCI DSS Requirements	Guidance
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	**Purpose** Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE.
	Good Practice All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams: • All locations, including retail locations, data centers, corporate locations, cloud providers, etc. • Clear labeling of all network segments. • All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version). • All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc. • Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism. • Date of last update, and names of people that made and approved the updates. • A legend or key to explain the diagram. Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.	

<table>
<tr><th></th><th>PCI DSS Requirements</th><th>Guidance</th></tr>
<tr><td rowspan="2">1.2.4</td><td>An accurate data-flow diagram(s) is maintained that meets the following:
Shows all account data flows across systems and networks.
Updated as needed upon changes to the environment.</td><td>Purpose An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices. Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured.</td></tr>
<tr><td colspan="2">Good Practice The data-flow diagram should include all connection points where account data is received into and sent out of the network, including connections to open, public networks, application processing flows, storage, transmissions between systems and networks, and file backups. The data-flow diagram is meant to be in addition to the network diagram and should reconcile with and augment the network diagram. As a best practice, entities can consider including the following in their data-flow diagrams:
All processing flows of account data, including authorization, capture, settlement, chargeback, and refunds.
All distinct acceptance channels, including card-present, card-not-present, and e-commerce.
All types of data receipt or transmission, including any involving hard copy/paper media.
The flow of account data from the point where it enters the environment, to its final disposition.
Where account data is transmitted and processed, where it is stored, and whether storage is short term or long term.
The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared.
Date of last update, and names of people that made and approved the updates.</td></tr>
</table>

Thus, each entity is tasked with maintaining 2 sets of diagrams: network diagrams and data flow diagrams. I use sets because there can be as many as needed to meet the intent of the requirements. The approach is to start from a high-level contextual diagram and add as many other diagrams as needed.

In PCI DSS 3.2.1 we had a minimum of 2 sets of network diagrams that had to be included: high-level network diagrams and detailed network diagrams. This was moved to a single section in PCI DSS 4.0 since the number of levels could vary wildly. Indeed, section 4.1 states that entities should:

- Provide one or more network diagrams that:
    - Shows all connections between the CDE and other networks, including any wireless networks.

- Is accurate and up to date with any changes to the environment.
- Illustrates all network security controls that are defined for connection points between trusted and untrusted networks.
- Illustrates how system components storing cardholder data are not directly accessible from the untrusted networks.
- Includes the techniques (such as intrusion-detection systems and/or intrusion-prevention systems) that are in place to monitor all traffic:
  - At the perimeter of the cardholder data environment.
  - At critical points in the cardholder data environment.

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.

So, we have 2 sets of diagrams. Let me detail the requirements that must be covered by each set (you can use this list as a checklist to validate your diagrams) including RoC section numbers from see table 1:

1. Network diagrams: to understand the entity's networking topography, showing the overall architecture of the environment being assessed, and how it connects to untrusted networks (those not under the entity's control, such as the internet)
   - Include all relevant network segments (both wired and wireless) where we find CDE and connected systems (with enough detail such as VLAN numbers and, potentially, IP ranges or a way to map it to ranges
     - networks that store, process and/or transmit Account Data (CHD and SAD) (the CDE)
     - networks that do not store, process and/or transmit Account Data, but are still in scope (segments containing connected systems that may also include out-of-scope systems)
     - wireless networks (regardless of whether the wireless network is a CDE)
     - networks confirmed to be out of scope
     - These are to be documented in section 4.5 In-scope Networks
   - Connections into and out of the network including demarcation points (devices that provide segmentation) at the boundaries between the CDE and other networks/zones (connected, wireless and wired networks, out-of-scope, untrusted)
   - Any segmentation points which are used to reduce the scope of the assessment (see section 3.2)
   - Critical components (hardware and software) within the CDE, including POS devices, systems, databases, and web servers, as applicable (see 4.8 In-scope System Component Types)
   - Third-party payment applications/solutions (4.4 In-scope Third-Party Service Providers)
   - Other necessary payment components, as applicable

- Connected entities for payment processing and transmission, including service providers and other third parties with which the entity shares cardholder data or that could affect the security of cardholder data (i.e. third parties and managed service providers)
- Data center facilities where any of the previously identified components are hosted

2. Data flow diagrams: to understand what data flows through which systems (and networks) - often, assessors ask clients to create business process diagrams (i.e. non technical) to describe how data is captured, stored (application level), shared or transmitted, and disposed. Business areas understand this easily. After this, we need to ensure that this is mapped over the applications, systems, networks and data center locations.
   - These must be overlaid over the network diagrams, or allow the assessor to easily see how they map over those (this often requires sitting down business owners, developers and network folks together)
   - They must cover the following data flows (described in section 4.2.1 Description of Account Data Flows of the RoC), generally using legends:
     - Authorization
     - Capture (refers to the specific transaction activity of data capture or entry into the network)
     - Settlement
     - Chargeback/Disputes
     - Refunds
     - Other as applicable (for example, authentication should be included)

   - For each type of data flow, the following information must be ascertained (often using legends on diagrams):
     - Types of Account Data (CHD and SAD) involved (for example, full track, PAN, expiration date)
     - Describe how cardholder data is transmitted and/or processed and for what purpose it is used (protocols, etc.)
     - Accompanying the diagrams with narratives for each flow is required (per section 4.2.1 Description of Account Data Flows of the RoC template)

   - Cardholder data storage locations (in section 4.3 Storage of Account Data of the RoC)

   - Note that sometimes having multiple diagrams for different flows (on top of the same diagrams) helps for legibility and maintainability of those diagrams
   - Data center facilities where any of the previously identified components are hosted

2A.2.3 Updates and validation of the consistency of the diagrams

All diagrams must be reviewed (some evidence of reviews must be kept, which may mean document that no changes were deemed needed) at least annually and when the environment changes significantly (both diagram requirements call for diagrams to be "kept current"). Requirement 6.5.2 mandates that "documentation is updated as applicable [...] [u] pon completion of a significant change".

It is the assessor's responsibility to ensure the consistency and completeness of the diagram sets and to document it in section 3.1 -Assessor's Validation of Defined Scope Accuracy-. This should generally follow requirement 12.5.2 which implies (and includes) validation of the diagrams to ensure that these actually accurately represent scope. The NSC (firewall) rules (ACLs) defined in requirement 1.2.5 and reviewed per requirement 1.2.7 should also follow in locked step.

2A.2.4 Legends and color coding

There are no requirements for using specific colors, so that detail is left to the entity (organization). What should be visually clear is what systems and network segments are CDE and connected systems. One common way is to use colors such as red for CDE systems and network, orange or yellow for connected systems or network, and green for anything out of scope (which is the color scheme I used in my model).

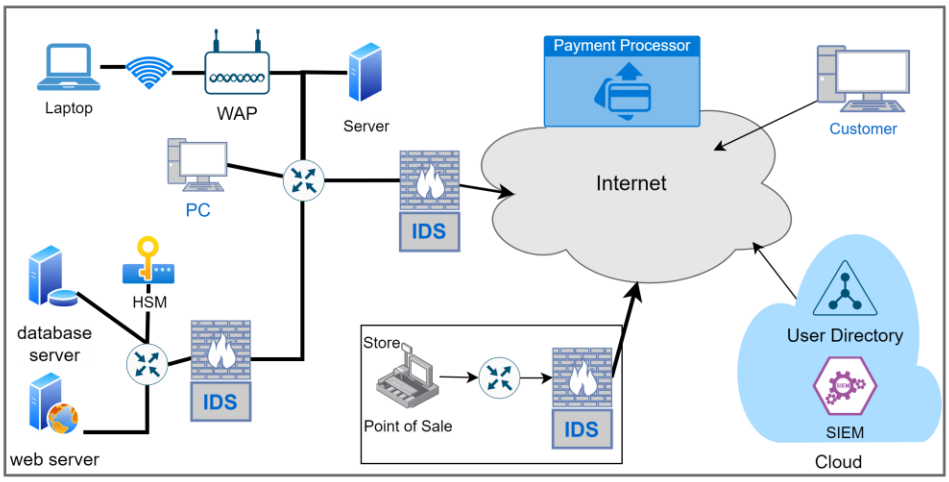
There should be a legend identifying icons and links on all the diagrams even if there are captions below the elements. The protocols linking system and network components need to be identified on the diagrams (for example, HTTPS, SFTP, TLS). Data flow diagrams should also indicate what elements of cardholder data (PAN, encrypted PAN, Expiration date, etc.) are sent over each data flow (which could be using legends).

I also now identify whether systems are SaaS/PaaS/IaaS (* aaS) where applicable since this impacts responsibilities over controls.

2A.2.5 Sample diagrams

The example diagrams are for a merchant with a store connected via the internet and a corporate office providing eCommerce payments. To simplify compliance, telephony in stores use standard phone lines and are not integrated in a networked-telephony system (phone networks are often forgotten - this is subject for other guidance). We are also not including any virtualization. These diagrams are but one possible representation. Styles may vary. Required content, much less so.

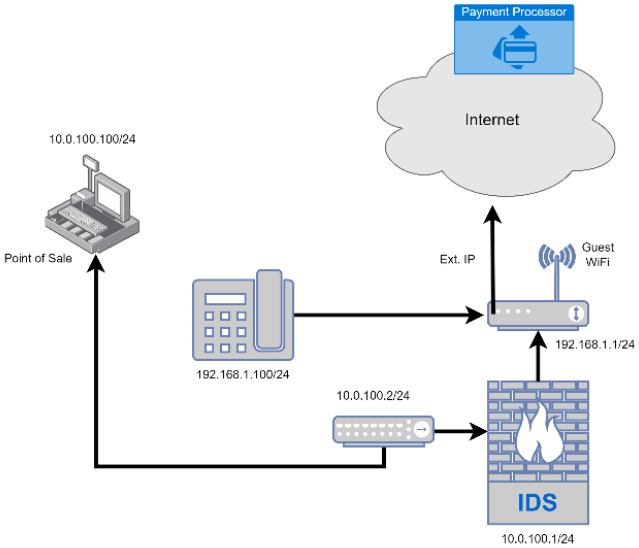
2A.2.5.1 Sample High-Level Diagram



Appendix 2A - Figure 1 - Sample High-Level Network Diagram

2A.2.5.2 Sample Detailed Network Diagram

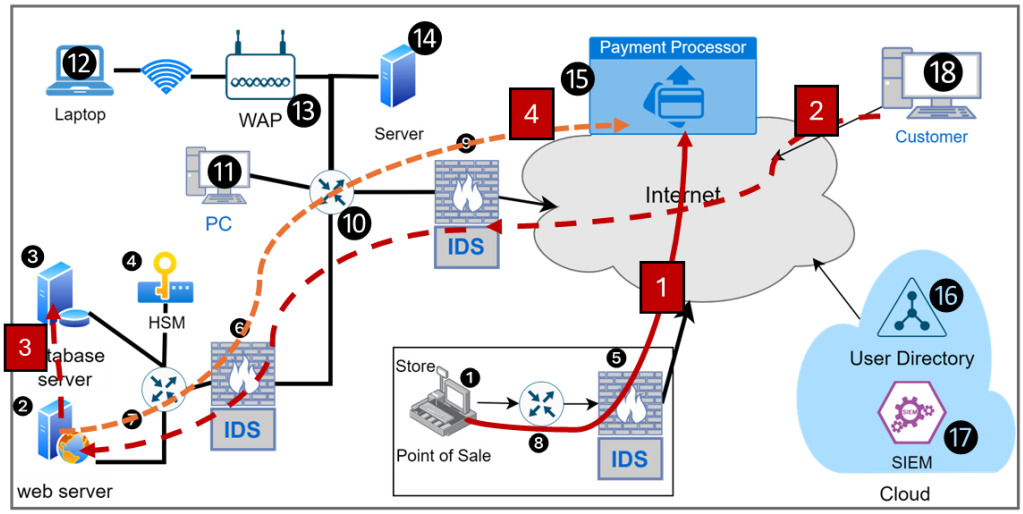
The example is of the store and includes IP addresses. We have the provided network range from the ISP (192.168.1.1/24) as well as an internal network range (10.0.100.0/24).



Appendix 2A - Figure 2 - Sample Detailed Network Diagram

2A.2.5.3 Sample Data-Flow Diagram

The data-flow diagrams (1.2.4) add flow information on top of the detailed network diagram. Elements that are irrelevant may be omitted. This example is for "capture" at a store or payment over the internet, where the customer's payment is processed. Other diagrams would be required in a real-world example. I often recommend that a textual narrative accompany the data flow diagrams (it ensures accurate understanding of the process).



Appendix 2A - Figure 3 - Sample Dataflow Diagram

Textual narrative of process/dataflow

Flows in the diagram (numbers in red boxes) :

- An end user pays with their payment card (card present payment) at the point of sale (1) in the store.
- The information will flow through the internal switch (8), through the firewall (5), through the internet, to the payment processor (15)
- The payment get processed via the payment networks, and the response is sent back.
- The customer's computer (18) (or mobile device) communicates over the internet through the external corporate firewall (9) coming into a switch (10) through the internal CDE firewall (6) up to the web server (2) to get processed.
- The customer browses the site, adds items to a card, and goes to checkout when ready to pay
- The payment data received by the web server (2) may be communicated to the database (3) if it is stored temporarily for whatever reason
- The payment data takes a similar reverse path to what it did from the customer, but going to the payment processor (15) through the internet and returning with the response.
- The result would be returned back to data flow number two [2].

2A.2.6 Complex cases

Sadly, we encounter many cases where things are not as simple as suggested in this document. While I cannot provide all possible examples, I do want to touch on points colleagues have raised regarding this.

2A.2.6.1 Authentication, Authorization and Auditing

PCI DSS includes requirements for user identification (section 8.2), authentication (section 8.3) and authorization (PCI DSS 7.*). Information security often refers to these as AAA, Authentication (including identification), Authorization and Auditing. Auditing, or monitoring, is part of requirement 10 in PCI DSS. Also now required for non-customer access is multifactor authentication (MFA, sections 8.4 and 8.5).

For simple environments, we can expect these authorizations are directly included in data flow diagrams. More complex environments may require specific diagrams that fully document authentication and other AAA functions for both privileged and non-privileged users in a logical and network/physical format.

2A.2.6.2 Composite & logical segmentation cases

Most times segmentation is accomplished through a simple mechanism such as layer 2 or 3 (see the OSI network model for details on these layers) NSC device such as a firewall or router (hence, the NSC configuration standards of requirement 1.2.1) which could be a physical or virtual device (slightly more complex).

Due to business or technical constraints some entities use a combination of processes and technology to achieve the equivalent segmentation. These cases are often not clearly documented and may require very detailed diagrams.

Web applications often use Application Programming Interfaces (API) methods to perform myriads of functions (from getting products and information, to payment). Logical segmentation may exist at the API levels, of between various groups of API (at layers 5 through 7 of the OSI model).

We can also have logical segmentation of filesystems or a system like SharePoint. For example, certain users of an organization may have a business need to have access to account data stored on organization servers. Here we'll likely need network segmentation of users (PCI and not) and logical segmentation of the server or systems.

Providing exact guidance is complex and we'd recommend you confirm more complex segmentation with your assessor as this falls outside the scope of this guidance (at this time).

End Notes - Volume 2A

[1] PCI Security Standards Council (2022, p.10). 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.