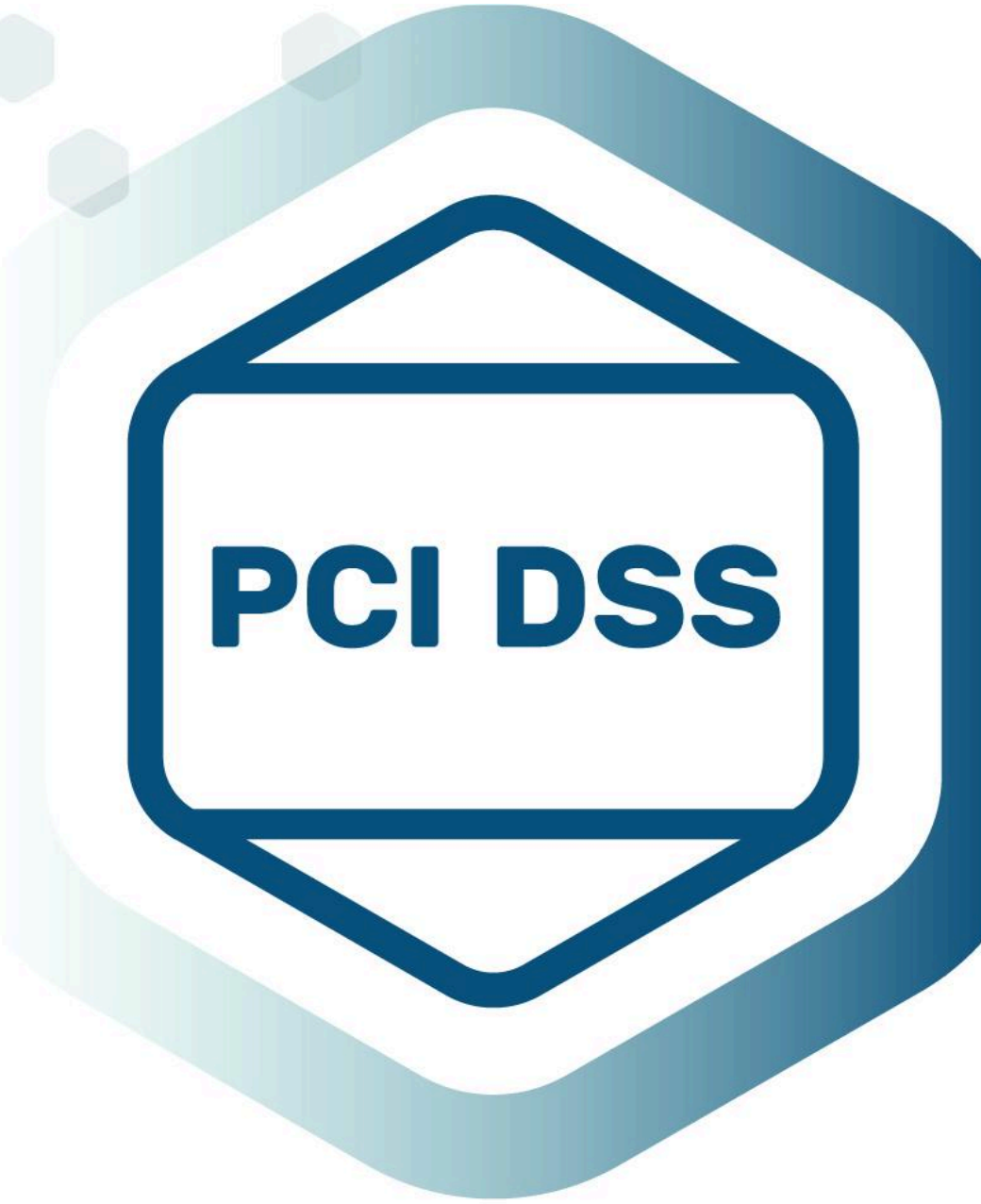


Scoping Toolkit

PCI DSS

Streamline and accelerate your PCI Scoping.

Sg Strike Graph

Introduction

Many organizations struggle to understand where PCI DSS controls are required, and which systems need to be protected.

This document provides guidance to help organizations identify the systems that need to be included in scope for PCI DSS.

In PCI v4, organizations are required to formally document their PCI DSS scope. Entities may use this template to help them document their scope.

When it comes to scoping for PCI DSS, the best practice approach is to start with the assumption that everything is in scope until verified otherwise. When properly implemented, network segmentation is one method that can help reduce the number of system components in scope for PCI DSS. Other methods may also be effective at reducing the number of systems to which PCI DSS controls apply and/or the size of the CDE such as outsourcing to a third-party service provider or using less risky payment acceptance methods such as iframe in an e-commerce environment or IVR systems in a telephony environment.

Key Terms

PCI DSS – Payment Card Industry Data Security Standard - A set of baseline technical and operational requirements designed to protect payment account data.

CDE – Cardholder Data Environment - The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

CHD – Cardholder Data - At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code

SAD – Sensitive Authentication Data - Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Account Data – Cardholder Data and/or Sensitive Authentication Data

Scoping process overview

1. **Identify how and where the organization receives CHD.**
   Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer

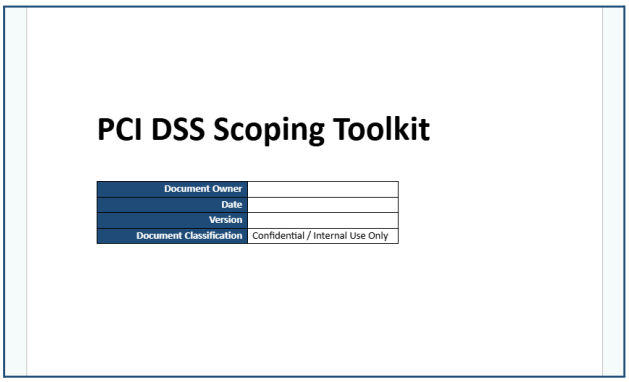
2. **Locate and document where account data is stored, processed, and transmitted.**
   Document all CHD flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE.

3. **Identify all other system components, processes, and personnel that are in scope.**
   Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These people, processes, and technologies are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD.

How to use this document

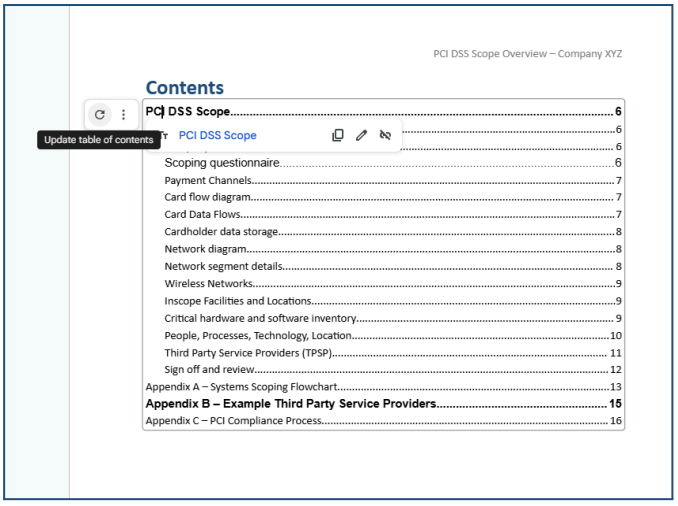
1. **Delete pages 1-3**
   Remove the Strike Graph branded pages and How-To pages of the document so that you can customize it for your company.

2. **Add your company branding**
   Place your company logo on the first page and/or in the header of the document, and change the information in the header and footer to fit your company.



3. **Populate document with your company information**
   Fill out the table forms and diagram fields as needed.

4. **Update the Table of Contents**
   Once your updates are complete, update the table of contents to match the structure of the final document.



PCI DSS Scoping Toolkit

Document Owner	
Date	
Version	
Document Classification	Confidential / Internal Use Only

Contents

Introduction **1**
Key Terms 2
Scoping process overview **2**
How to use this document **3**
Contents **5**
PCI DSS Scope **6**
Company Details 6
Company Overview 6
Scoping questionnaire 6
Payment Channels 7
Card flow diagram 7
Card Data Flows 7
Cardholder data storage 8
Network diagram 8
Network segment details 8
Wireless Networks 9
Inscope Facilities and Locations 9
Critical hardware and software inventory 10
People, Processes, Technology, Location 11
Third Party Service Providers (TPSP) 12
Sign off and review 13
Appendix A – Systems Scoping Flowchart **14**
Appendix B – Example Third Party Service Providers **16**
Appendix C – PCI Compliance Process **17**

PCI DSS Scope

Company Details

Company name:	
Company address:	
Company URL:	
Company contact name:	
Company phone number:	
Company email address:	

Company Overview

Describe the nature of the business:	
Describe how you store, process and/or transmit cardholder data:	
Types of payment channels:	☐Internet/Ecommerce ☐POS/Card-Present ☐Telephone Order/Call Centre ☐Mail Order ☐Other:
Other relevant details:	

Scoping questionnaire

Question	Comment
Cardholder data (CHD) storage	
Is CHD ever electronically stored?	
If so, how is it protected?	
Are hashes and masked/truncated PANs (full card numbers) ever stored together?	
Is Sensitive Authentication Data (SAD) (pin or cvv/cvc) ever stored?	
Is any cardholder data ever retained on paper?	
Is there any legacy storage of CHD?	
Ecommerce	
Does the business have an ecommerce channel(s)?	
What type of integration methods are used?	
Are third parties used to develop sites?	
Are third parties used to host sites?	
Do any third parties have access to or maintain the webservers/environment?	
Do you develop or support ecommerce for other entities?	
Card present	
Are card present payments taken?	
What type of terminal connection?	
Are they currently PTS approved?	
What is the make and model of the devices?	
Is a P2PE solution used?	
Are imprint (click clack/zip zap) machines used to take card payments?	
Phone	
Is cardholder data ever taken over the phone?	
If so VOIP or POTS?	
Are calls recorded?	
Are DTMF Masking or IVR solutions used?	
Miscellaneous	

Is any card data received via email?	
Is any card data received via fax?	
Is card data ever sent via email??	
Is any card data received via post or courier?	
Are any virtual terminals used to process payment data?	
If VT is used, is the machine segmented from other systems?	
Are any payment applications developed in-house used to process card data?	

Payment Channels

Payment Channel	Description	Owner	SAQ Scope	Comments

Card flow diagram

Insert diagram or reference

Last reviewed date:

Card Data Flows

Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer.

- Identify 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
    4. file backups.
- Confirm 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.
- Ensuring account data flow diagrams are updated and accurate.
- For any account data found outside of the currently defined CDE, the entity either 1) securely deleted it, 2) migrated it into the currently defined CDE, or 3) expanded the currently defined CDE to include it.

#	CHD flow purpose	Description	Transport	Protection	CHD types (PAN, CVV, PIN, Expiry)
1	Capture				

2	Authorization				
3	Authorization				
4	Authorization				
5	Settlement				
6	Chargeback				

Add and remove rows as needed.

Cardholder data storage

Data store (database, folder, cloud)	File(s) and/or table(s)	CHD elements stored (PAN, Expiry, Name, SAD)	Method to secure (Encryption strength, hashing algorithm, tokenization, access controls, truncation)	How access is logged.

Network diagram

Insert diagram

Last reviewed date:

Network segment details

Identify all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.

Describe all networks that store, process, and/or transmit Account Data:

Networks that store, process, and/or transmit CHD (in scope)		
Network Name	**Function/purpose of the network**	**Description of any segmentation controls**

Describe all networks that do not store, process, and/or transmit Account Data but are still in scope—for example, connected to the CDE or provide management functions to the CDE, etc.:

Connected-to / security impacting networks (in scope)

Network Name	Function/purpose of the network	Description of any segmentation controls

Describe all networks confirmed as out of scope including segmentation controls and justification.

Out-of-scope networks		
Network Name	**Function/purpose of the network**	**Description of any segmentation controls and justification of the network being out of scope.**

Is segmentation used to reduce scope of PCI **(yes/no)**	
If segmentation is used identify the supporting processes:	

Wireless Networks

Wireless Network	Used to store, process, or transmit CHD?	Connected to the CDE?	Could impact the security of the CDE?	Confirmed out of scope?

Inscope Facilities and Locations

Identify and provide details for all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers and mail rooms) in scope. Add rows, as needed.

Facility Type (Datacenters, corporate office, call center, mail processing facility, etc.)	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (for example, city, country)
Example 1: Data center	1	Los Angeles, California, United States
Example 2: retail locations	132	92 locations in the United States and 40 in Canada

Critical hardware and software inventory

Identify all types of system components in scope.

"System components" include network devices, servers, computing devices, virtual components, cloud components, and software. Examples of system components include, but are not limited to:

- Systems that store, process, or transmit account data (for example, payment terminals, authorization systems, clearing systems, payment middleware systems, payment back-office systems, shopping cart and store front systems, payment gateway/switch systems, fraud monitoring systems).
- Systems that provide security services (for example, authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems (for example, badge access or CCTV), multi-factor authentication systems, anti-malware systems).
- Systems that facilitate segmentation (for example, internal network security controls).
- Systems that could impact the security of account data or the CDE (for example, name resolution, or e-commerce [web] redirection servers).
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Cloud infrastructure and components, both external and on-premises, including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, CDEs residing on-premises or in the cloud, service meshes with containerized applications, and container orchestration tools.
- Network components, including but not limited to network security controls, switches, routers, VoIP network devices, wireless access points, network appliances, and other security appliances.
- Server types, including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices.
- Printers, and multi-function devices that scan, print, and fax.
- Storage of account data in any format (for example, paper, data files, audio files, images, and video recordings).
- Applications, software, and software components, serverless applications, including all purchased, subscribed (for example, Software-as-a-Service), bespoke and custom software, including internal and external (for example, Internet) applications.
- Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the CDE or to systems that can impact the CDE.

For each item, even if they reside with other system components, list them below with each component with different roles, vendors, or make/model/version on separate rows. Add rows as needed.

Type of System Component	Total Number of System Components	Vendor	Product Name and Version	Role/Function Description

Fill table or provide a link to the asset inventory

People, Processes, Technology, Location

People	Processes	Technology	Locations
Examples: ● *Cashiers and sales clerks* ● *Back-office clerks* ● *Call center operators* ● *Systems and network administrators* ● *IT support personnel* ● *Application developers* ● *Key custodians* ● *Human resources* ● *Information security officers* ● *Physical security officers* ● *Customer support* ● *Accounting/finance personnel* ● *Supervisors/managers for each area* *Senior management and executives*	*Examples:* ● *Regular payment processing channels* ● *Payment cancellations and chargebacks* ● *Back-up and fail-over processes* ● *Reconciliation, periodic reporting* ● *Distribution and storage of paper reports and other physical media* ● *Legacy processes and data stores* ● *Onboarding processes for new personnel* ● *Authorizations and approvals for system access* ● *Firewall review processes* ● *Change management* ● *Scheduling of security patch deployments* ● *System building and configuration* ● *Identifying and escorting visitors* ● *Performing log reviews* ● *Processes for reporting potential security incidents* *Security policy updates*	*Examples* ● *Servers, applications, networks, devices* ● *Physical security systems* ● *Logical security systems* ● *Payment terminals and point of sale systems* ● *Electronic communications* ● *Backups and disaster recovery "hot" sites* ● *Telecommunications* ● *POTS vs. VoIP* ● *Management systems* ● *Remote access systems* *Cloud technology*	*Examples:* ● *Sydney head office* ● *Melbourne data centre* ● *Brisbane secure destruction site* *Adelaide call centre*

Third-Party Service Providers (TPSP)

Third parties that cardholder data is shared with or who could affect the security of cardholder data must be handled in accordance with PCI DSS. Examples of TPSPs include: payment gateways, hosting providers, development support, etc. For a larger list of examples see Appendix B – Example Third-Party Service Providers (TPSPSs)

Identify all connections from third-party entities with access to the CDE.

Company Name	Is cardholder data shared?	How can the company impact the security of CHD?	PCI DSS Compliance status	Does the third party connect to the CDE, if so how?

Sign off and review

I have identified 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).

I have updated all data-flow diagrams per Requirement 1.2.4.

I have identified 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.

I have identified all system components in the CDE, connected to the CDE, or that could impact security of the CDE.

I have identified all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.

I have identified all connections from third-party entities with access to the CDE.

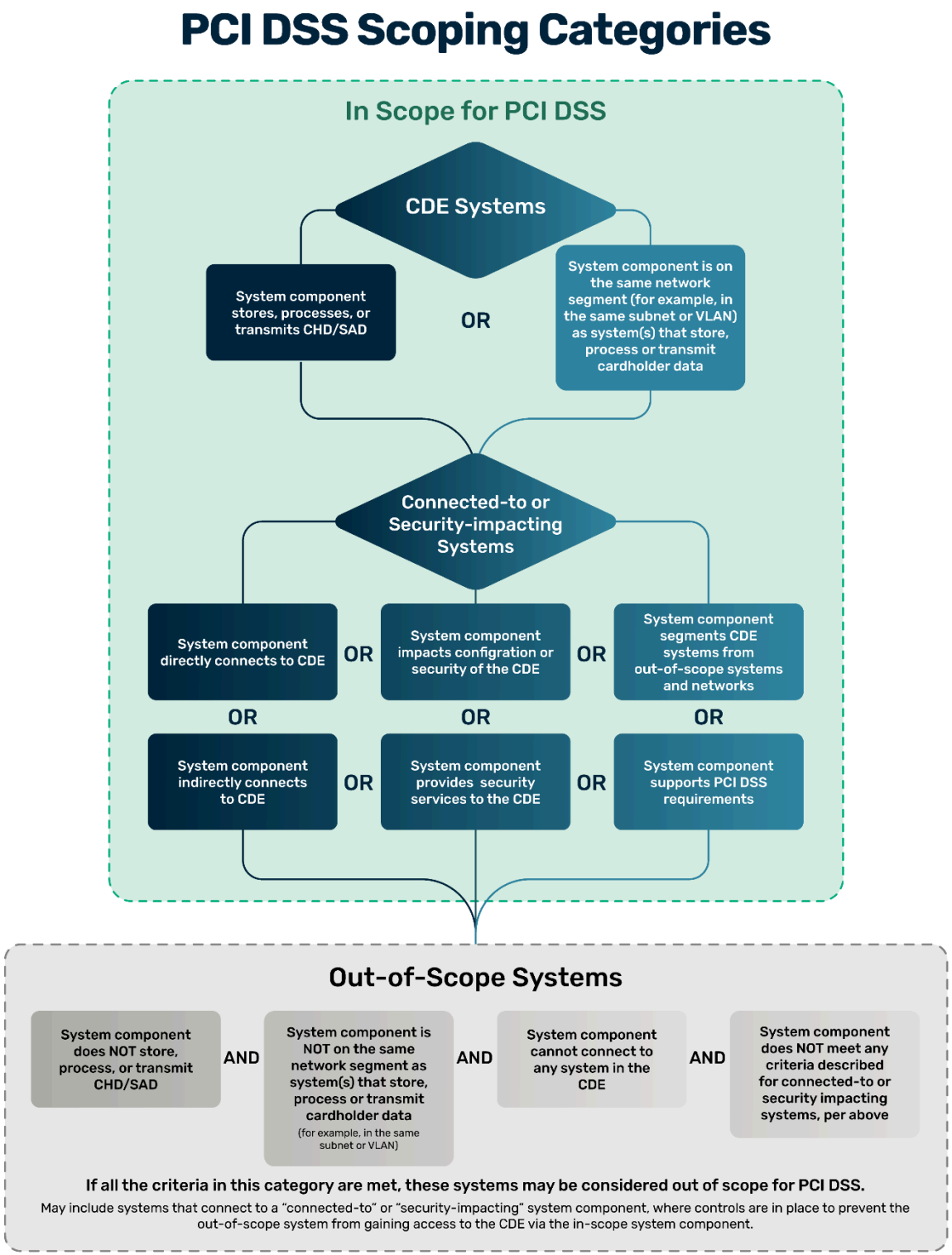
I confirm that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

I confirm that this scope will be reviewed annually (or biannually for Service Providers) and upon any significant change to the environment. I understand that all changes to the scope must be communicated to executive management (Last requirement is for Service Providers only).

Compliance Program Sponsor: _____ Date: _____

Signature: _____

Appendix A – Systems Scoping Flowchart



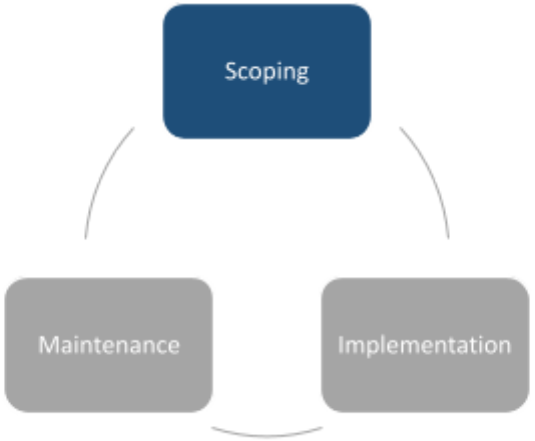
System Type	Description	Scope and Applicability
CDE Systems	• System component stores, processes, or transmits CHD/SAD. OR • System component is on the same network segment—for example, in the same subnet or VLAN as system(s) that store, process, or transmit CHD/SAD.	**These systems**: • Are in scope for PCI DSS. • Must be evaluated to determine the applicability of each PCI DSS requirement.
Connected-to and/or Security Impacting Systems	• System component is on a different network (or subnet or VLAN), but can connect to or access the CDE (e.g., via internal network connectivity). OR • System component can connect to or access the CDE via another system—for example, via connection to a jump server that provides access to the CDE). OR • System component can impact configuration or security of the CDE, or how CHD/SAD is handled— for example, a web redirection server or name resolution server. OR • System component provides security services to the CDE—for example, network traffic filtering, patch distribution, or authentication management. OR • System component supports PCI DSS requirements, such as time servers and audit log storage servers. OR • System component provides segmentation of the CDE from out-of-scope systems and networks—for example, firewalls configured to block traffic from untrusted networks	**These systems**: • Are in scope for PCI DSS. Even where a connection is limited to specific ports or services on specific systems, those systems are included in scope to verify that the applicable security controls are in place. • Must be evaluated to determine the applicability of each PCI DSS requirement. • Must not provide an access path between CDE systems and out-of-scope systems.
Out-of-scope systems	• System component does NOT store, process, or transmit CHD/SAD. AND • System component is NOT on the same network segment or in the same subnet or VLAN as systems that store, process, or transmit CHD. AND • System component cannot connect to or access any system in the CDE. AND • System component cannot gain access to the CDE nor impact a security control for CDE via an in-scope system. AND • System component does not meet any criteria described for connected-to or security-impacting systems, per above	**Out-of-Scope Systems:** • Are not in scope for PCI DSS; therefore PCI DSS controls are not required. • Have no access to any CDE system; if there is any access, then system is in scope. • Are considered untrusted (or "public")—there is no assurance they have been properly secured. • If on the same network (or subnet or VLAN) as, or otherwise has connectivity to, a connected-to or security impacting system, controls must be in place to prevent the out-ofscope system from gaining access to the CDE via the inscope systems. These controls must be validated at least annually.

Appendix B – Example Third Party Service Providers

Below are examples of types of services and providers with which an entity may work:

- Organizations involved in the storage, processing, and/or transmission of cardholder data (CHD). Thirdparty service providers in this category may include:
  - Entities providing call center and customer contact services
  - E-commerce payment providers
  - Organizations that process payments on behalf of the entity, such as a partner or reseller
  - Fraud verification services, credit reporting services, collection agencies
  - Third-party processors
  - Entities offering processing-gateway services
  - Third-party debt collectors/collection processes
- Organizations involved in securing cardholder data. TPSPs in this category may include:
  - Companies providing secure destruction of electronic and physical media
  - Secure storage facilities for electronic and physical media
  - Companies that transform cardholder data with tokenization or encryption
  - E-commerce or mobile-application third parties that provide software as a service
  - Key-management providers such as key-injection services or encryption-support organizations (ESO)
- Point-of-sale companies (or integrators/resellers) involved with installation, maintenance, monitoring, or otherwise support of their systems.
- Organizations involved in the protection of the cardholder data environment (CDE). TPSPs in this category may include:
  - Infrastructure service providers
  - Managed firewall/router providers
  - Secure data-center hosting providers
  - Monitoring services for critical security alerts such as intrusion-detection systems (IDS), antivirus, change-detection, compliance monitoring, audit-log monitoring, etc.
- Organizations that may have incidental access to CHD or the CDE. Incidental access is access that may happen as a consequence of the activity or job. TPSPs in this category may include:
  - Providers of managed IT delivery channels and services
  - Companies providing software development, such as web applications
  - Providers of maintenance services—for example, HVAC or cleaning services

Appendix C – PCI Compliance Process



Stage	Activity	Description
Scoping	Identify how and where the organization receives CHD.	1. Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer
	Locate and document where account data is stored, processed, and transmitted.	2. Document all CHD flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE.
	Identify all other system components, processes, and personnel that are in scope.	3. Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These people, processes, and technologies are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD.
Implementation	Implement controls to minimize scope to necessary components, processes, and personnel.	4. Implement controls to limit connectivity between CDE and other in-scope systems to only that which is necessary. 5. Implement controls to segment the CDE from people, processes, and technologies that do not need to interact with or influence the CDE
	Implement all applicable PCI DSS requirements	6. Identify and implement PCI DSS requirements as applicable to the in-scope system components, processes, and personnel.
Maintenance	Maintain and monitor.	7. Implement processes to ensure PCI DSS controls remain effective day after day. 8. Ensure the people, processes, and technologies included in scope are accurately identified when changes are made.