State of Arizona

State Treasurer’s Office

Annual PCI Scoping Exercise

About this Document

To properly assess a cardholder data environment's compliance with the Payment Card Industry Data Security Standard (PCI DSS), it is important to understand the scope of the merchant or service provider's cardholder data environment. PCI DSS requires that merchants and service providers perform a scoping exercise annually to ensure they understand the people, processes, and technologies that comprise their cardholder environment, on which PCI DSS controls must be enforced. The purpose of this exercise is to help guide and document the annual scoping exercise performed by the Security Metrics, a contracted PCI QSA by the State Treasurer's Office.

Table 1 - Revision History

Version	Date	Author	Description of Change
0.1			Process document creation

Contents

Introduction

To safeguard the State of Arizona's cardholder data environment and to protect the confidentiality of customer data, including cardholder data, requirements of the Payment Card Data Security Standard (PCI DSS) must be enforced on all systems that store, process, or transmit data, or that can affect the security of these systems. To ensure PCI controls have been properly implemented within the cardholder data environment, it is important to have a clear understanding of the people, processes, and technologies that make up the State of Arizona's cardholder data environment.

The PCI DSS requires all merchants or service providers who receive, process or store cardholder data, or who can affect the security of a merchant's cardholder data to perform a scoping exercise at least annually to ensure a proper understanding of the scope of the cardholder data environment.

Purpose / Scope

The primary purpose of this document is to guide the organization through a thoughtful and thorough review of their cardholder data environment. If the organization does not understand the extent and scope of their cardholder environment, they will not be able to properly protect it. This guide is to be used in conjunction with the PCI Security Standards Council's Information Supplement titled "Guidance for PCI DSS Scoping and Network Segmentation."

When scoping a cardholder environment, it is recommended to begin with the assumption that everything is in scope and work to validate that proper segmentation is in place to remove systems or network segments from scope. While segmentation is not required to be compliant with PCI DSS, proper segmentation can help to reduce the cost of maintaining compliance.

Scoping Exercise Responsibilities

The State Treasurer's Office is the assigned custodian(s) of this scoping guide and responsibilities for performing and documenting the annual scoping review. It is the responsibility of the custodian(s) of this scoping guide to publish and disseminate outcomes of the annual scoping exercise to State of Arizona management and relevant system administrators to ensure PCI DSS requirements have been applied to all systems and processes determined to be within the PCI scope. This process document will also be reviewed at least annually by the custodian(s) (and any relevant data owners) and updated as needed to reflect changes to the PCI DSS or the risk environment.

Questions or comments about this policy should be directed to the custodian(s) listed above.

Description of the Environment

Provide a brief description of the nature of the Merchant/Service Provider's business.

1 Description of how Cardholder Data is Received, Processed or Stored

Provide a brief description of how cardholder data is received (all input channels), processed and stored. Description should include all people, processes, and systems involved in the payment flow.

1.2 Cardholder Data Input Channels

Cardholder data is received via the following input channels:

- ☐ Card-Present
- ☐ E-Commerce
- ☐ Mail order/telephone order (MOTO)
- ☐ Email
- ☐ Fax
- ☐ Other

2 Cardholder Data (CHD) Flows

Table 2.1 – Description of all cardholder data flows in the environment.

Cardholder Data Flows	Types of CHD Involved (e.g., full track, PAN, expiry)	Describe how cardholder data is transmitted and/or processed
Capture		
Authorization		
Settlement		
Chargeback		
Identify all other data flows, as applicable (add rows as needed)		
Other (describe)		

Glossary of Terms:

Capture: Describes any mechanism by which you gather or acquire cardholder data. This includes entry into web forms/E-commerce sites, Call Centers (MOTO), card-present physical swipe on a magnetic stripe reader (MSR), fax, etc.

Authorization: Occurs when a merchant sends the card data outbound, usually to the payment processor or payment gateway, and then receives transaction approval after the acquirer authorizes the transaction with the issuer/processor.

Settlement: All transactions are not final for processing or payment until settlement, which occurs when all credit card transactions have been closed. For example, some point-of-sale systems store cardholder data in the form of batch files. Usually, a batch begins with the first transaction of the business day, and ends with

the last transaction of the day before the batch is closed (settled). During settlement, a report is electronically submitted to the processor finalizing the day's sales as complete. Funds are deposited in the merchant's account usually 48 business hours after the batch settlement. In table 2.1 above, indicate if any cardholder data is sent to the processor as part of this settlement process.

Chargeback: Describe any scenario where cardholder data may be used or viewed in any chargeback process. Chargeback or dispute resolution is performed when a customer disputes a change on their credit card. Chargeback requests are typically sent to the merchant by the acquiring bank or by the card brand (e.g., American Express) directly.

PAN: Primary Account Holder

CHD: Card Holder Data

Note: additional flows may be included in this table. If other flows exist in the environment, they should be added to the "other category" and described effectively. "Other" flows can include processes such as Issuing, Call Recording, end-of-day report generation, archiving, etc.

2.1 Card Data Flow Diagrams

For each card data flow noted in table 2.1 above, include a cardholder data flow diagram along with a brief written description of the cardholder data flow. Cardholder data flow diagrams should depict all systems involved in the cardholder data flow. The diagrams should have sufficient details to allow viewers to determine which elements of cardholder data (PAN, CVV, track, etc.) pass through or are stored on company systems.

2.2 Cardholder Data Storage

The following table identifies all databases, tables, and files storing cardholder data and provides details on controls in place to protect stored cardholder data and to log access to said data.

Table 2.2 – Description of cardholder data storage environment.

Data Store (file, table, etc.)	**Cardholder data elements stored** (PAN, expiry, any elements of SAD)	**How data is secured** (for example, use of encryption, access controls, truncation, etc.)	**How access to data stores is logged** (description of logging mechanism used for logging access to data—for example, enterprise log management solution, application-level logging, operating system logging, etc.)

2.3 Cardholder Data Environment Network Segments

Table 2.3.1 – Describe all networks that store, process and/or transmit cardholder data:

Network Name (in scope)	Function / Purpose of Network

Table 2.3.2 – Describe all networks that do not store, process or transmit cardholder data, but are connected to or can affect the security of systems that do transmit, process, or store cardholder data. Due to their connections to systems in the cardholder data environment and their ability to affect the security of systems that transmit, process, or store cardholder data, these systems are considered in scope and all applicable PCI controls must be in place.

Network Name (in scope)	Function / Purpose of Network

Table 2.3.3 – Describe any networks confirmed to be out of scope. These are network segments that have no connectivity (inbound or outbound) from systems in the cardholder data environment (listed in 2.3.1). Network segmentation tests (PCI DSS Requirement 11.3.4) must be performed to verify complete segmentation from these network zones and the CDE network zones.

Network Name (out of scope)	Function / Purpose of Network

2.4 Inventory of Hardware and Software

2.4.1 – The following tables contain an inventory of all hardware (servers, firewalls, appliances, etc.) and software (payment applications, antivirus, FIM, logging, etc.) involved in the storage, transmission, or processing of cardholder data. This also includes all systems on the same network segment as systems directly

involved in the storage, processing, or transmission of cardholder data (systems listed in network zones from table 2.2.1).

Table 2.4.1.a – Inventory of all systems (servers, workstations, laptops, etc.) in the CDE.

System Inventory	Hardware Vendor Make and Model (indicate if a virtual appliance	OS Type & Version	All Assigned IP's or range of IP's for groups of similar workstations.	Role / Functionality	Qty

Table 2.4.1.b – Inventory of all network components in the CDE.

Network Components	Firmware Version	Hardware Vendor Make and Model	OS Version	Assigned IP's	Role/Functionality
e.g., VPN Appliance					
Firewall					
RSA Authentication Server					
IDS / IPS					
Etc.					

Table 2.4.1.c – Inventory of all payment applications in the CDE.

Name of Third-Party Payment Application/Solution	Version of Product	PA-DSS validated? (yes/no)	P2PE validated? (yes/no)	PCI SSC listing reference number	Expiry date of listing, if applicable

Table 2.4.1.d – Inventory of critical applications in the CDE.

Name of Software/Application	Version or Release	Role/Functionality

2.4.2 – The following table contains an inventory of all hardware (servers, firewalls, appliances, etc.) and software (IDS/IPS, antivirus, FIM, logging, etc.) for systems that are connected to or can affect the security of the cardholder data environment (systems listed in network zones from table 2.2.2).

Table 2.4.2.a – Inventory of all systems (servers, workstations, laptops, etc.) connected to or which can affect the security of the CDE. These are systems which do not transmit, process, or store cardholder data directly, but can affect the security of systems which store, process, or transmit cardholder data (Active Directory servers, antivirus servers, log servers, etc.).

System Inventory	Hardware Vendor Make and Model (indicate if a virtual appliance)	OS Type & Version	All Assigned IP's or range of IP's for groups of similar workstations.	Role / Functionality	Qty

Table 2.4.2.b – Inventory of all applications installed on systems that are connected to or can affect the security of the CDE. This includes critical management and security systems (Active Directory, logging, antivirus, patching, etc.).

Name of Software/Application	Version or Release	Role/Functionality

2.5 Connected Entities

Merchants and service providers are responsible for transmissions of cardholder data from their environments to other third-party providers (payment gateways, payment processors, fraud detection services, etc.). As part of the annual scoping exercise, the State Treasurer's Office must verify all transmissions of cardholder data to third parties have been properly documented and assessed.

Table 2.5 – Connected entities for processing or transmission of cardholder data.

Identify All Processing Entities (Acquirer / Bank / Brands)	Directly Connected? (yes/no)	Reason(s) for Connection:	
		Processing	Transmission
		☐	☐

		☐	☐
		☐	☐
		☐	☐

2.6 Third-Party Service Providers

Table 2.6 – Lists all third-party service providers with whom cardholder data is stored or who provide services that can affect the security of the cardholder data environment. These entities are subject to PCI DSS Requirement 12.8.

Company Name	**What data is shared** (for example, PAN, expiry date, etc.)	**The purpose for sharing the data** (for example, third-party storage, transaction processing, etc.)	**Status of PCI DSS Compliance** (Date of AOC and version #)

2.7 People and Departments of the Cardholder Data Environment

Table 2.7 – Defines individuals and departments involved in the acquisition, processing, and storage of cardholder data. This table also includes IT resources responsible for configuring and securing CDE systems and key custodians responsible for managing encrypted storage of cardholder data.

Individual or Department	**Description of user role in the acquisition, transmission, storage, or security of cardholder data**

3 Remote Access

Any system with access into the CDE can potentially affect the security of cardholder data. Remote access to the CDE must be carefully controlled and reviewed to ensure proper controls are in place to allow access without compromising the security of the CDE. Remote access to the CDE from network zones considered to be out-of-scope (Table 2.3.3) should be required to access the CDE via a system that is part of the reviewed scope (Table 2.3.2) and not CDE systems directly. Multi-factor authentication (PCI DSS Requirement 8.3) is also required for any remote access to the CDE.

Table 3.1 – Remote access review.

Individual or Group with Remote Access	What CDE systems can be accessed remotely and why	Protocol in use (RDP, VPN, SSH, etc.)	Description of Multi-Factor authentication in place to protect remote access

4 Scope Reduction Controls

When scoping a cardholder environment, it is recommended to begin with the assumption that everything is in scope and work to validate that proper segmentation is in place to remove systems or network segments from scope. During this scoping exercise <insert your agency name> has determined that adequate segmentation is in place between the cardholder data environment and the systems within the network zones indicated in Table 2.3.3 above. The following security controls were verified to provide adequate segmentation from the CDE to these out-of-scope networks:

Describe scope reduction controls in place to remove network segments from PCI scope. Scope reduction controls may include firewalls configured to block all traffic to and from out-of-scope network to the CDE, complete air-gap segmentation, or other controls. Describe the controls in place and testing performed to verify segmentation is working appropriately. Testing segmentation must include at a minimum annual penetration testing on any device responsible for performing segmentation of the CDE.