Effectively Scoping PCI Assessments
Introduction

One of the most important activities in a Payment Card Industry Data Security Standards (PCI DSS) assessment is to determine the scope of the assessment. A PCI DSS Qualified Security Assessor (QSA) is responsible for validating that a client’s PCI scope is accurate and complete. Many organizations struggle to demonstrate which systems need to be protected. It is up to the QSA to properly guide and evaluate the methods and procedures the client used to determine their PCI scope.

This exercise is a critical aspect to any PCI assessment and sets the foundation for how the QSA will determine which controls are in scope and how they will be assessed. This whitepaper provides guidance to both QSAs and clients on how to effectively scope a PCI assessment, while highlighting best practices.

PCI DSS Scoping Fundamentals

According to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms, v3.2, April 2016, the definition of scoping is the following:

“Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.”

Opinions vary on how to determine what is in scope for a PCI DSS assessment. Here are some key activities and concepts to use to help narrow down what truly is in scope in a client environment:

- Identify where and how the organization receives cardholder data (CHD).
- Identify where CHD is stored, processed, or transmitted.
- Identify personnel who can interact with or influence the cardholder data environment (CDE).
- Identify system components that reside in or connect to the CDE.

Identifying system components that are in scope tends to be a challenge for clients to identify, therefore the Payment Card Industry Security Standards Council (PCI SSC) provided logical guidance to help QSAs and clients categorize what systems should be in scope for a PCI DSS assessment. As referenced in the Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation, v1.1, May 2017, the PCI SSC broke down systems components into 3 main categories:

- **CDE Systems** – These are system components that either store, process, or transmit CHD or SAD (Sensitive Authentication Data), or a system component that is on the same network segment as systems that store, process, or transmit CHD/SAD.

- **Connected-To or Security Impacting Systems** – There are number of scenarios that apply to this category, and if a system component fits any one of the below criteria, it will be considered in scope for a PCI DSS assessment:
  - A system component directly connects to a CDE system, OR...
  - A system component indirectly connects to a CDE system, OR...
  - A system component impacts the configuration or security of a CDE system, OR...
  - A system component provides security services to the CDE, OR...
  - A system component supports a PCI DSS requirement.

- **Out-of-Scope Systems** – There are a number of scenarios that apply to this category. If a system component meets all of the criteria below, it will be considered out-of-scope for a PCI DSS assessment:
  - A system component does not store, process, or transmit CHD/SAD, AND...
  - A system component is not in the same network segment as systems that store, process, or transmit CHD/SAD, AND...
  - A system component cannot connect to any system in the CDE, AND...
  - A system component does not meet any of the criteria listed above for connected-to or security-impacting systems.
Best Practices to Validate PCI DSS Scope

There are several methods organizations should use to effectively determine the PCI DSS scope that follow a QSA’s standardized approach to ensure scope accuracy:

1. **Identify Inventory** – Prepare the most current hardware and software inventory for the QSA. This is required to be maintained as a PCI DSS requirement that the QSA will ask for during the onset of the scope analysis. (PCI DSS Requirement 2.4: Maintain an inventory of system components that are in scope for PCI DSS).
   a. Ensure the inventory has been documented and kept current, and ensure it lists all hardware and software components in-scope for the assessment.

2. **Network and Data Flow Diagrams** – Ensure the network and data flow diagrams are current and up-to-date and compare to the inventory. It is a PCI DSS requirement to keep these current. (PCI DSS Requirement 1.1.2 and 1.1.3).
   a. Ensure that system components depicted on the diagrams align to the hardware/software inventory list.

3. **Identify List of People In-Scope** – Document a list of personnel in-scope to the assessment. This will include roles such as System Admin, Network Admin, Security Personnel, Call Center and Data Center Personnel, and any other role that connects to or works in the defined CDE.

4. **Identify Storage of CHD** – Prepare a list of all systems that store CHD, onsite or offsite.
   a. Knowing exactly where cardholder is stored is important to understand. Those systems should be included in the hardware/software inventory list.

5. **Document Method to Discover Existence of CHD** – It is important to understand the discovery methods to determine where CHD is located, especially CHD that could reside outside the defined cardholder data environment. Clearly document the methods that were used to ensure no cardholder exists outside the CDE, such as specific types of tools used, scanning tools, manual checks and observations or a combination of each.

6. **Segmentation** – Examine firewall rules to ensure the CDE is clearly segmented from out-of-scope systems. Careful review of the firewall rules will also help a QSA understand what is allowed to connect into the CDE. Any system that connects into the CDE is considered in-scope to the PCI DSS assessment.

**Conclusion**

There are many moving elements when considering the scope of a PCI DSS assessment. The QSA and the client each play an important role in determining and validating PCI DSS scope. One of the key aspects to successfully validating PCI DSS scope is for the QSA and client to foster a collaborative partnership. Understanding each role helps the QSA and client work together towards a common goal to efficiently navigate the assessment process.

**Why Kratos**

Kratos has years of robust compliance and certification experience with government and commercial standards and compliance frameworks requirements. As one of the first and largest Federal Risk and Authorization Management Program (FedRAMP) 3PAOs, Kratos’ compliance experience also includes CMMC (C3PAO), Payment Card Industry (PCI), Federal Information Security Management/Modernization Act (FISMA) and the National Institute of Standards & Technology (NIST) Risk Management Framework (RMF). Because of this experience, Kratos is viewed as a trusted compliance and governance partner by the Department of Defense (DoD), Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.

As a Payment Card Industry Security Standards Council (PCI SSC) approved Qualified Security Assessor Company (QSAC), Kratos provides PCI Data Security Standards (PCI DSS) advisory and assessment services across all payment channels for merchants and service providers who access, process, transmit or store credit card transactions or provide a security function to an entity’s cardholder data environment. Our QSAs are seasoned professionals and ready and willing to assess your PCI DSS scope and provide expert guidance to successfully navigate through the assessment process.

Contact us for a free consultation to see how we can serve your PCI DSS validation needs.
CyberSales@KratosDefense.com