Many companies leverage Third-Party Service Providers (TPSP) to achieve or maintain PCI DSS compliance. TPSPs store, process, or transmit Cardholder Data (CHD) on the entity’s behalf or provide a security function to the entity’s Cardholder Data Environment (CDE). As a result, these TPSPs effectively extend the entity’s boundary of responsibility, adding an additional layer of accountability for ensuring that the CHD or CDE are appropriately secure and adhere to PCI DSS requirements. This whitepaper provides best practices to effectively manage the use of TPSPs to ensure that CHD and CDE systems are secure and protected in a PCI DSS compliant manner.

Understanding the Service Provider Layers

It’s important to understand the difference between an entity that is undergoing a PCI DSS compliance assessment, and the relationship of the service providers used to help achieve PCI DSS compliance. These service providers may also leverage other service providers to assist the entity to achieve PCI DSS compliance.

**Entity:** “Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.”

**Service Provider:** “Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.”

**Nested or Chained TSP:** “Any entity that is contracted for its services by another third-party service provider for the purposes of providing a service.”

With multiple layers of TPSPs, many entities can struggle with identifying which service providers are in scope for their PCI DSS assessment, as well as what their responsibilities are for the use, security, and assessment involvement of TPSPs who process, store, transmit, and protect their cardholder data and environment.

**Best Practices to Identify PCI DSS In-Scope TPSPs**

If an entity can answer yes to any of the below questions for each TPSP they use, the TPSP is in-scope for their PCI DSS assessment.

1. Will the TPSP store, process, or transmit CHD?
2. Will the TPSP be involved in the protection or access to CHD?
3. Will the TPSP be involved in the protection or access to the CDE?
4. Will the TPSP have incidental access to the CDE?

The first critical step of a robust third-party assurance program to manage PCI DSS TPSPs is to identify the services provided by the TPSPs.

---

1 According to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms, v3.2, April 2016
2 According to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms, v3.2, April 2016
PCI DSS Requirements for TPSPs

The PCI DSS Report on Compliance (ROC) clearly outlines the requirements an entity must demonstrate in relation to how TPSPs need to be managed. These requirements are mandatory for each TPSP in-scope to an entity’s PCI DSS assessment:

- **12.8.1** – Verify that a list of service providers is maintained and includes a list of the services provided.
  - *QSA Evidence Tip:* This requirement is looking for an inventory list of service providers that clearly articulate the services provided by each in-scope TPSP. Most entities either leverage a procurement inventory system to produce this evidence or use a spreadsheet that lists each TPSP and the services they provide. Either is acceptable as long as it is updated on an annual basis. Using version control mechanisms help prove that the list is being maintained and kept current.

- **12.8.2** – Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE.
  - *QSA Evidence Tip:* Many entities use contracts and service agreements to satisfy this control requirement. Entities must ensure that the contract or service agreement contains relevant language that suggests and/or requires TPSPs to be responsible for the security of CHD or the entity’s CDE. The contract or service agreement does not have to be verbatim to 12.8.2 but must adhere to the spirit and context of the control.

- **12.8.3** – Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
  - *QSA Evidence Tip:* This control requires an entity to have a TPSP management program that evaluates and reviews TPSPs prior to using them for PCI DSS services. Entities must be able to demonstrate the due diligence practices used to ensure TPSPs meet their standards. Most entities use a program or spreadsheet that lists out various control questions and criteria to evaluate whether the TPSP meets their corporate and information security requirements. During a PCI DSS assessment, the QSA will review the output of those evaluations for each in-scope TPSP.

- **12.8.4** – Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.
  - *QSA Evidence Tip:* The QSA will be looking for a formal, signed, and current PCI DSS Attestation of Compliance (AOC) for each in-scope TPSP. This could either be a full assessment Service Provider AOC or a Service Provider SAQ-D.

- **12.8.5** – Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
  - *QSA Evidence Tip:* The QSA will be looking for a formal Responsibility Matrix that clearly outlines which PCI DSS requirements the TPSP is responsible for, and which ones the entity is responsible for. A Responsibility Matrix must be in place for each in-scope TPSP.

- **12.9 Additional requirements for service providers only** – Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.
  - *QSA Evidence Tip:* For those TPSPs going through their own PCI DSS assessment, they must provide evidence that they communicated to their “customer” their responsibilities for securing their CHD or CDE. Many TPSPs include this language in their contracts or service agreements.
What to do if a TPSP does not have a valid or current AOC or SAQ-D

Many opinions vary amongst QSA Companies on how to broach this topic. There are several steps that a QSA may take to ensure a TPSP is PCI compliant and/or meets the intent of PCI DSS requirements. According to the example given by the PCI SSC, three key questions should be asked of each in-scope TPSP:

1. Does the TPSP have validated PCI DSS compliance for the entity’s specific services?
2. Does the TPSP have evidence to prove the requested service meets the intent of PCI DSS requirements?
3. Does the TPSP have an outstanding project goal to become PCI DSS compliant?

If the entity cannot answer yes to all three questions, the PCI SSC recommends that the entity select another TPSP. This hard line does not always make sense in the business world. Therefore, QSAs and entities need to agree on how best to validate that a TPSP meets the intent of PCI DSS requirements for that entity’s PCI DSS assessment.

One approach includes requesting validation documentation from the TPSP for the relevant PCI DSS controls. In essence, this entails including a representative from the TPSP in the entity’s assessment. This is not a popular approach as it tends to increase the assessment timeline. This is why the PCI SSC recommends using TPSPs that undergo their own PCI DSS validation assessments. The entity is accountable for ensuring TPSPs are compliant to PCI DSS requirements. If the TPSP cannot demonstrate compliance, the entity and the QSA are responsible for validating the TPSP meets PCI DSS requirements. When these situations arise, it is important for the entity to work closely with their QSA to determine the best approach for validating a TPSP environment. Start with network and dataflow diagrams, and work from there to identify relevant systems in scope. Once the scope of that TPSP has been confirmed, the QSA can determine which PCI DSS controls are relevant for that TPSP and ask for evidence accordingly. After the assessment is completed, it is strongly recommended to work toward requiring that particular TPSP to perform their own PCI DSS assessment to ease the level of effort in the next assessment cycle.

Conclusion

The Information Supplement: Third-Party Security Assurance, v1.1, March 2016 contains detailed guidance from the PCI SSC on how to handle the due diligence process of TPSPs, and it is recommended to review that document thoroughly. Understanding the role and importance of TPSPs and how they are used and managed is a critical function in achieving and maintaining PCI DSS compliance. There is a tremendous need to have a robust third-party assurance program in place to ensure that company standards and information security policies and procedures are adhered to, which will help entities safeguard their PCI cardholder data environments and cardholder data they collect, process, transmit, and store on behalf of their customers.

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.

Joseph Scarzone – Kratos PCI Capability Lead
CyberSales@KratosDefense.com