Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Date: March 2016

Author: Third-Party Security Assurance and Shared Responsibilities Special Interest Groups
PCI Security Standards Council

Information Supplement:
Third-Party Security Assurance

Document Changes

Date	Document Version	Description	Pages
August 2014	1.0	Initial release	All
March 2016	1.1	Expanded and revised content based upon the Shared Responsibilities Special Interest Group	Various

Table of Contents

1 Introduction

As entities work toward the goal of achieving and maintaining ongoing PCI DSS compliance, they may choose to leverage third-party service providers (TPSPs) to achieve their objectives. Entities can use a TPSP to store, process, or transmit cardholder data on the entity's behalf, or to manage components of the entity's cardholder data environment (CDE), such as routers, firewalls, databases, physical security, and/or servers. These TPSPs can become an integral part of the entity's cardholder data environment and impact an entity's PCI DSS compliance, as well as the security of the cardholder data environment.

The use of a TPSP, however, does not relieve the entity of ultimate responsibility for its own PCI DSS compliance, or exempt the entity from accountability and obligation for ensuring that its cardholder data (CHD) and CDE are secure. Clear policies and procedures should therefore be established between the entity and its TPSP(s) for all applicable security requirements, and proper measures should be developed to manage and report on the requirements.

A robust and properly implemented third-party assurance program assists an entity in ensuring that the data and systems it entrusts to TPSPs are maintained in a secure and compliant manner. Proper due diligence and risk analysis are critical components in the selection of any TPSP.

This guidance focuses primarily on the following:

Third-Party Service Provider Due Diligence: Thorough vetting of candidates through careful due diligence, prior to establishing a relationship, assists entities in reviewing and selecting TPSPs with skills and experience appropriate for the engagement.

Service Correlation to PCI DSS Requirements: Understanding how the services provided by TPSPs correspond to the applicable PCI DSS requirements assists the entity in determining the potential security impact of utilizing TPSPs on the entity's cardholder data environment. This information can also be used to determine and understand which of the PCI DSS requirements will apply to and be satisfied by the TPSP, and which will apply to and be met by the entity.

Note: *Ultimate responsibility for compliance resides with the entity, regardless of how specific responsibilities may be allocated between an entity and its TPSP(s).*

Written Agreements and Policies and Procedures: Detailed written agreements promote consistency and mutual understanding between the organization and its TPSP(s) concerning their respective responsibilities and obligations with respect to PCI DSS compliance requirements.

Monitor Third-Party Service Provider Compliance Status: Knowing the TPSP's PCI DSS compliance status helps to provide the organization engaging a TPSP with assurance and awareness about whether the TPSP complies with the applicable requirements for the services provided. If the TPSP offers a variety of services, this knowledge will assist the entity in determining which TPSP services will be in scope for the entity's PCI DSS assessment.

1.1 Intended Use

The intent of this information supplement is to provide guidance to entities engaging TPSPs with whom CHD is shared or that could impact the security of CHD, as required by PCI DSS Requirement 12.8[1]. This additional guidance for PCI DSS Requirement 12.8[1] is intended to assist entities and TPSPs better understand their respective roles in meeting this requirement.

The information in this document is intended as supplemental guidance and does not supersede, replace, or extend PCI DSS requirements. Ultimately, the entity is responsible for ensuring its own PCI DSS compliance, whether or not a TPSP is involved. How responsibilities are allocated between an entity and its TPSP(s) often depends on the specific relationship and services being provided. This guidance does not replace proper risk assessment, and compliance with the guidance does not guarantee compliance with Requirement 12.8[1], etc.

1.2 Terminology

The following terms are used throughout this document:

- **Entity** – An entity is any organization that has the responsibility to protect card data and may leverage a third-party service provider to support them in card-processing activities or to secure card data.
- **TPSP (Third-party Service Provider)** – As defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*, a service provider is a 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. There are many types of businesses that could fall into the category of "service provider," dependent on the services provided. Most commonly, a TPSP could be a legally separate entity; but it can also be a separate business unit or component of the entity under assessment—for example, an internal service provider—where the provider is outside the direct management control of the entity assessed.
- **Nested or Chained TPSP** – A nested or chained TPSP is any entity that is contracted for its services by another third-party service provider for the purposes of providing a service.

1.3 Audience

Entities Engaging a Third-Party Service Provider (for example, issuers, merchants, acquirers, or other service providers) – Entities that engage TPSPs for the storage, transmission, processing of cardholder data, or otherwise provision of services that control or may impact the security of cardholder data may benefit from these guidelines. The recommendations provided in this document are intended to assist entities in developing an increased understanding regarding utilization of TPSPs and the subsequent impact to the entity's cardholder data environment, the impact to the entity's own PCI DSS compliance responsibilities, as well as provide guidance on how to meet the intent of PCI DSS Requirement 12.8[1] governing TPSPs.

[1] This reference is to PCI DSS v3.1 – April 2015

Third-Party Service Providers – This guidance document may also provide useful information for TPSPs in understanding the responsibilities of TPSPs to the entities for which the TPSPs are providing services. In addition, a TPSP may be dependent on the compliance of a nested or chained TPSP to achieve overall compliance of a service. The TPSP should understand how best to engage with its partner(s) to ensure PCI DSS compliance of the services being offered. PCI DSS Requirement 12.9[2] also requires service providers to acknowledge in writing to the TPSP's customers its responsibilities for securing the customers' cardholder data or the customers' cardholder data environment.

Acquirers (also known as "acquiring banks," "merchant banks," or "acquiring financial institutions") – As an entity that initiates and maintains relationships with merchants for the acceptance of payment cards, an acquirer is responsible for ensuring that the merchants in its portfolio are using secure TPSPs.

[2] This reference is to PCI DSS v3.1 – April 2015

2 Examples of Third-Party Service Providers

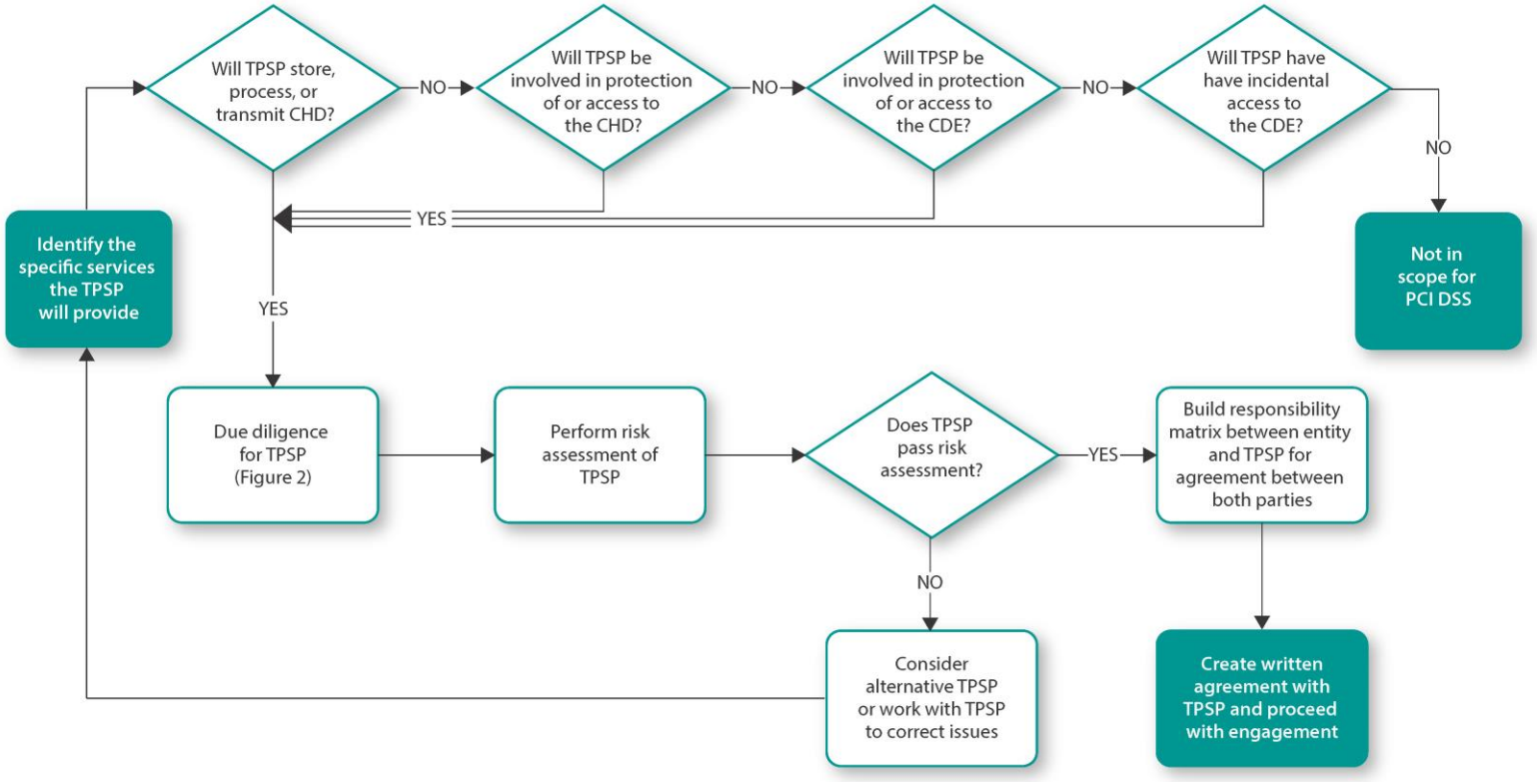
Below are examples of types of services and providers with which an entity may work:

- Organizations involved in the storage, processing, and/or transmission of cardholder data (CHD). Third-party 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), anti-virus, 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

3 Third-Party Service Provider Due Diligence

Partnering with the right TPSPs is a challenging task. Initial considerations should include measures to protect cardholder data, financial data, and other sensitive and personal data, and complying with local laws and regulations. Each organization should develop its own policies and procedures, as well as its own criteria for pre-selecting and managing potential TPSPs during the vetting process. All efforts should be placed on exerting the appropriate amount of due diligence and performing a risk assessment of pre-selected TPSPs. Below is an example of a high-level process flow that an entity may include as part of its due diligence when engaging TPSPs. Please note this process is not exhaustive. It is meant as a guideline to assist organizations in creating an appropriate due diligence program to engage TPSPs.

Figure 1: High-level TPSP Engagement Process



3.1 Determining the Scope of the Services Provided

When engaging a TPSP, initially, the entity should consider determining the scope of the TPSP's involvement with regard to storing, processing, or transmission of cardholder data and the resulting effect on the security of the CDE. Because TPSP involvement and services may impact the level of risk assumed by the entity when processing payment transactions, thorough due diligence is critical in determining which TPSP is appropriate and which third-party services may be needed.

Defining the level of involvement of a TPSP is crucial to understanding the overall risk assumed by the entity related to PCI DSS compliance. The entity may elect to engage an outside party to assist with the assessment of the scope of services to be provided by the TPSP and the applicability of those services to the entity's PCI DSS compliance. Questions that may help with this process include:

- Given the current payment ecosystem and payment channels, what services (security, access, etc.) would affect or impact the CDE and/or CHD? How are the services structured within the TPSP facilities?
- What technology and system components are used by the TPSP for the services provided?
- Are additional third parties used by the TPSP in the delivery of the service provided?
- What other core processes/services are housed in the TPSP facilities that may impact the services provided? What technology is used for those core processes/services?
- How many facilities does the TPSP have where CHD is or will be located?

Note: *The scope and services to be provided by a TPSP will depend on the specific facts and circumstances and services provided. Although the foregoing list of questions may be useful in determining scope and services, this list is not exhaustive. Each organization seeking to engage a TPSP must determine what is relevant in light of the circumstances, the organization's payment environment, the proposed TPSP's role, and other factors determined to be important through thorough due diligence.*

3.2 Due Diligence Research of the Third-Party Service Provider

Based on services provided by the TPSP, the entity will need to determine a due diligence path to identify the impact a TPSP has on the entity's PCI DSS scope. The entity should consider beginning with a preliminary review of the TPSP to ensure that the engagement does not negatively impact the entity's PCI DSS compliance. This research may include precautions such as consulting with the acquirer, reviewing the participating payment card brand service-provider listings and websites, and requesting PCI DSS validation documentation. Please note not all payment card brands have service-provider listings; however, some payment card brand rules require certain types of service providers to be registered with the payment card brand. Additional risk considerations (that may be outside the scope of PCI DSS requirements) include assessing the TPSP's:

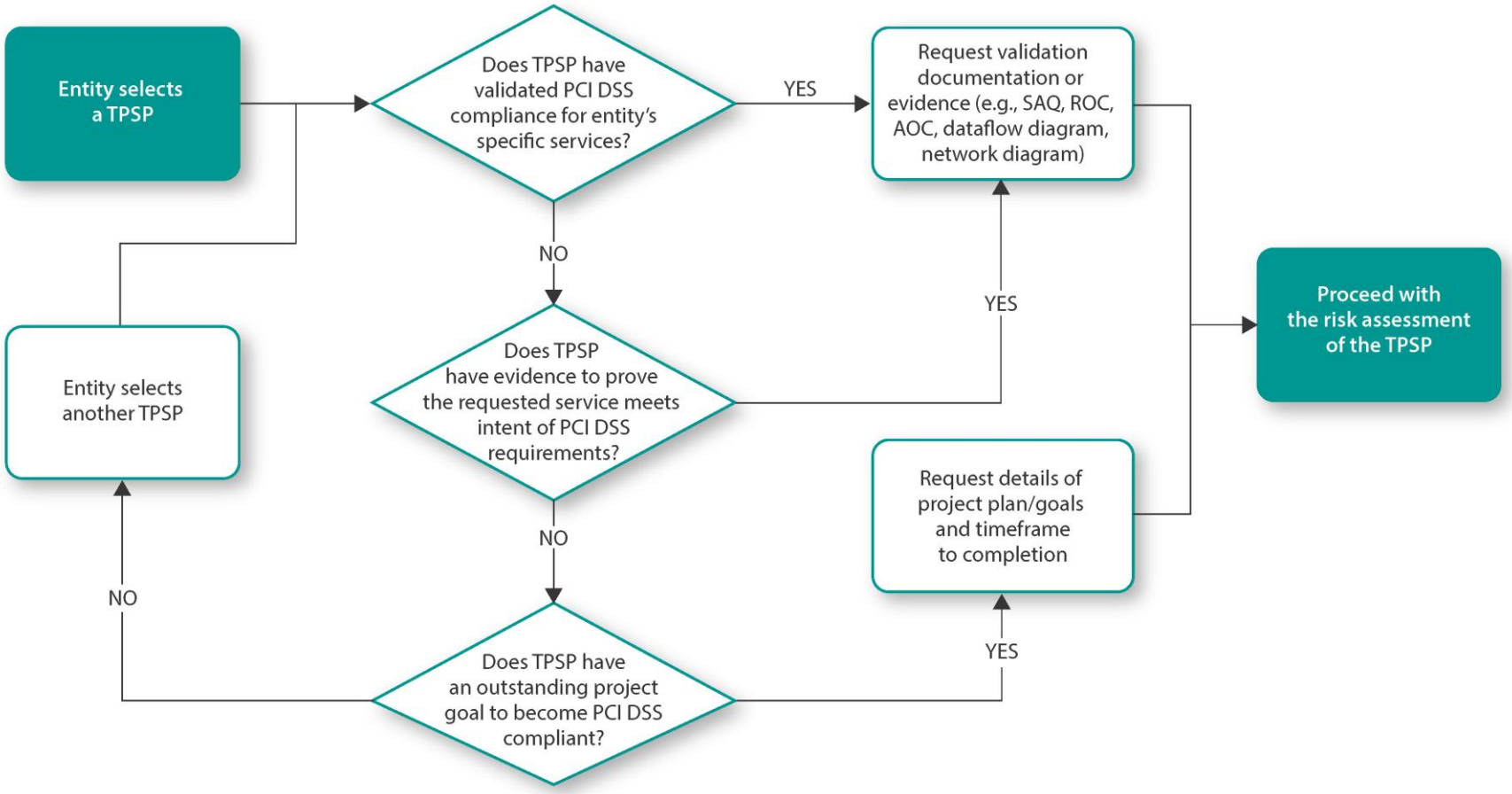
- Financial stability prior to contract execution or renewal
- Reputation, including the review of reported complaints and litigation
- Experience in providing or implementing the proposed services, including the TPSP's ability to

maintain service over time and management experience

- Insurance coverage
- Use of nested TPSPs to provide the requested services and assessment of nested TPSPs' ability to perform such services
- Compliance with your organization's third-party security policies
- Breaches, if they occurred, and the remediation status of each breach
- Business continuity preparedness
- Consideration of any potential legal risk

The workflow diagram in Figure 2 below details one potential high-level flow for an organization to follow when performing due diligence research on potential TPSPs. As noted above, however, each organization must determine the appropriate due diligence process in light of its own CDE. Part of that due diligence will include a decision on what form of evidence of the TPSP's compliance with the PCI DSS will be acceptable both initially and throughout the term of the relationship.

Figure 2: Example of Due Diligence Process



Entities may need to consult with their acquirer or payment card brand to determine if there are any requirements for engaging a TPSP. See Section 3.2.1 for more information.

3.2.1 Acquirer/Payment Card Brands

As part of the due diligence process and prior to continuing with the research, an entity may also wish to inquire with its acquirer or payment card brand[3] to ensure the TPSP services are approved for use by the acquirer or payment card brand and that there are no restrictions regarding which TPSPs can be used. In some cases an acquirer or payment card brand may disallow the engagement of TPSPs due to risk that has already been previously identifed

3.2.2 Third-Party Service Provider Validation Documentation

The entity may also consider requesting validation documentation from the TPSP that demonstrates the TPSP has achieved PCI DSS compliance. How and whether a TPSP must validate PCI DSS compliance is defined by the payment card brands, and required validation documentation may vary. This, in turn, impacts the types of compliance documentation an entity can expect to receive from the TPSP. Refer to the payment card brands' websites for more information about specific brand compliance programs, or contact the payment card brands directly.

The level of documentation should be commensurate with the level of risk and impact the TPSP presents to the entity's PCI DSS compliance. The documentation should be sufficient to confirm that the services provided are covered by the TPSP's PCI DSS assessment, and identify the PCI DSS requirements that were assessed to be in place. The documentation should also include information related to any services provided by the TPSP in other countries.

Accordingly, an entity that is required to validate its compliance through a full onsite assessment can rely on the self-assessed validation of its TPSP—if that TPSP is eligible to self-assess and if this is in line with the organization's risk management position and the applicable payment brand compliance programs.

As part of the due diligence process, the following documentation, as applicable, may be obtained from TPSPs that have been validated as PCI DSS compliant. The list also contains recommendations for reviewing validation documentation that may be provided to the entity. Validation documentation being provided to the entity should cover the service(s) being delivered by the TPSP to the entity to help ensure the services provided are covered by the TPSP's compliance validation:

- **Report on Compliance (ROC):** Completed by either an Internal Security Assessor (ISA) or by an external Qualified Security Assessor (QSA). Relevant sections of the ROC may be sufficient to demonstrate the scope of a PCI DSS assessment and compliance status. This may be unnecessary if the AOC covers the required services.
    - If compensating controls are used, determine why the original requirement could not be met; understand what the control is, how it is meeting the intent and rigor of the original requirement, and how the control is being maintained.

Note: *It is possible that a TPSP may choose not to share certain aspects or any portion of its ROC if sensitive information is included or where releasing the document may compromise confidentiality. Alternative information may include a redacted ROC to protect any confidential information, a remote*

[3] Payment card brand contact information can be found on the PCI SSC website: https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands

session where sensitive information can be reviewed when required, or a face-to face meeting to allow for viewing of the documentation. Additionally, many QSAs provide a letter on company letterhead, which may be used if the TPSP does not want to share potentially confidential information contained in its ROC.

- **Attestation of Compliance (AOC):** Fully executed "Attestation of Compliance for Onsite Assessments – Service Providers"[4] may be provided to the entity upon request. Template and information to complete the document can be found on the PCI SSC website.
  - Examine the name and type of services assessed found in Section 2A, "Scope Verification," to validate the services provided by the TPSP are covered. Examples are "Hosting Provider" and "Payment Processing."
  - Review relationships with other TPSPs to understand whether there are any additional services that may need evaluation or inclusion.
  - Review the AOC to determine whether the TPSP has requirements that are non-compliant that should be covered by the services provided.
  - Careful review of Part 2G, "Summary of Requirements Tested," is warranted as it contains those PCI DSS requirements the TPSP has fully tested, partially tested, or not tested for each service provided. For any "Partial" or "None" responses, the entity should review to ensure the services provided are covered. If the service provided was not covered by this assessment, the entity may wish to include this in its PCI DSS assessment. Note that PCI DSS requires the assessed entity to maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity (Requirement 12.8.5[4]). Please be aware, however, that PCI DSS does not require the TPSP to account for all PCI DSS requirements (for example, using a compliance matrix for all its customers).
- **Self-Assessment Questionnaire (SAQ) D and Attestation of Compliance for Service Providers (AOC):** Completed by TPSP if completing a self-assessment. These documents can be found on the PCI SSC website.
  - Careful review of Part 2G, "Summary of Requirements Tested,"[4] is warranted as it contains those PCI DSS requirements the TPSP has fully tested, partially tested, or not tested for each service provided. For any "Partial" or "None" responses, the entity should review to ensure the services provided are covered. If the service provided was not covered by this assessment, the entity may wish to include this in its PCI DSS assessment.
  - If compensating controls are used, determine why the original requirement could not be met; understand what the control is, how it is meeting the intent and rigor of the original requirement, and how the control is being maintained.
  - Appendix D of the SAQ, if provided, may be reviewed to understand which requirements are marked as non-applicable or not tested to know whether they are acceptable and clearly explained.

[4] Refers to version 3.1 – April 2015

- If provided, review Part 2E, "Description of Environment"[5], and Part 2D, "Payment Application"[5], to determine whether they are included in the assessment for the services provided.
- Review Section 3, "Validation and Attestation Details"[5], to confirm the results of the assessment.

▪ **ASV Scan Report Attestation of Scan Compliance (AOSC):** Provided by the TPSP's Approved Scanning Vendor if the TPSP is providing services that are delivered via systems required to meet PCI DSS Requirement 11.2.2[6]. Information about the AOSC is provided within the *PCI DSS ASV Program Guide,* available on the PCI SSC website. As with the ROC, the AOSC may be redacted to remove sensitive or confidential information.

- AOSC may be reviewed for the compliance status, scan expiration date, and number of identified failing vulnerabilities in order to determine whether the particular services are covered in these scans and have passed the scan.

All previous documentation may also have the validation dates tracked with periodic updates from the TPSP. The entity should also ensure all prior non-compliant issues with the TPSP have been remediated, if the remediation timeline has passed.

As these various documents are requested from compliant TPSPs, the entity should also consider requesting written verification that the services being provided to the organization fall within the scope of the services covered by the AOC, ROC, SAQ, and AOSC. This provides an additional measure of assurance that the TPSP's PCI DSS assessment is aligned with the agreed-upon services. Developing validation checklists may ensure key fields of the AOC, SAQ, ROC, or AOSC are reviewed by the management team.

If the TPSP has not attained PCI DSS compliance due to an outstanding gap in its environment, it is the responsibility of the entity to determine whether or not to accept the risk of engaging that TPSP. It is recommended the entity first understand what gap the TPSP must address in order to establish compliance and the impact of that gap to its own environment. If it is determined there is an impact, the entity should establish a clear and effective plan to remediate the issues. Among other things, this may include requesting project timelines and goal milestones from the TPSP to determine whether compliance can be achieved for the services offered, within a timeframe acceptable to the entity. Once the scope and gap have been identified, an entity may need to consult with its acquirer to ensure there is no conflict with the engagement.

***Note**: Some payment card brands require certain types of service providers to validate PCI DSS compliance. Per payment card brand rules, for certain types of services, only those service providers who are listed and deemed PCI DSS compliant may be used.*

If the TPSP does not intend to validate PCI DSS compliance or is not required to validate PCI DSS compliance and the entity still elects to engage the TPSP, the entity will be required to cover the applicable TPSP systems and processes under its own PCI DSS compliance assessment. The following

[5] Refers to SAQ D version 1.1 – July 2015
[6] This reference is to PCI DSS v3.1 – April 2015

are examples of documentation the TPSP may provide during a PCI DSS assessment, whenever significant changes occur, and/or annually, as applicable:

- A high-level dataflow diagram showing how the TPSP's services interface with the entity's environment
- Network diagrams
- Evidence of system-patching methodology and, if applicable, secure coding methodology
- List of the entity's TPSPs and how each TPSP is connected to the entity's environment, along with the role the TPSPs play—specifically, any chained/nested relationships
- Results of the TPSP's internal and external vulnerability scans, if available
- Security policies and operational procedures

If the TPSP is not yet compliant, it may provide its own project plan for its PCI DSS compliance path project plan or a copy of its Prioritized Approach for the service(s) provided, if available. The Prioritized Approach is a tool produced by PCI SSC to help entities implement PCI DSS requirements in a prioritized order that effectively addresses the respective risks. The tool may be downloaded from the PCI SSC's Document Library at https://www.pcisecuritystandards.org/security_standards/documents.php.

Another scenario to consider is if an entity engages a third party to augment the entity's information technology or operational staff, using only the entity's own processes and technology. In such a case, the third-party staff augmentation firm will likely not be independently assessed for its compliance with PCI DSS. However, the third-party employees embedded within the entity's in-scope processes may need to be part of the entity's own compliance validation exercise. This could include demonstrating that they follow the entity's own procedures, have their work reviewed by the entity's management, and are subject to all the same security controls as the rest of the entity's staff—such as, but not limited to, background checks, security awareness training, and secure-coding training.

The entity may also wish to consider the risk associated with engaging with a TPSP and how to limit the exposure to the entity's PCI DSS scope. In addition, the entity may wish need to consider the additional effort associated with validating and potentially remediating the applicable system components and processes that fall into scope. For example, the entity may weigh its risk and time impact to perform an internal assessment of the TPSP's systems and processes vs. hiring an external resource to audit the TPSP system on behalf of the entity. Ultimately, because the TPSP has not validated its compliance, the services provided may be in scope for the entity's PCI DSS assessment and subsequently may result in a delay to the entity's compliance validation.

3.2.3 Payment Card Brand Validated Providers Lists and Websites

Payment card brands may maintain lists of validated TPSPs that satisfy specific brand enrollment programs, which typically include requirements to attain and maintain PCI DSS compliance. It is important for an entity to understand the scope of such the validation and the services listed. Please note that absence of a TPSP from a list does not preclude an engagement of the service provider, since some TPSPs choose not to be listed, although they have attained PCI DSS compliance. Similarly, the inclusion of a service provider on a published list does not by itself provide assurance that the services applicable

to the entity's engagement are included in the compliance validation, or that all PCI DSS requirements that an entity wishes the TPSP to manage on its behalf are included in the validated service. Depending on the services provided by the TPSP to the entity, the information found on the payment card brand service provider listings may not provide the necessary assurance. Additional information may be needed from the TPSP for the services provided.

3.3 Perform Risk Assessment

It is recommended an entity perform a thorough risk assessment on its TPSP based on an industry-accepted methodology. Understanding the level of risk associated with engaging a TPSP will help the entity in its decision-making process. An entity may need to create a tiered due diligence program with decision trees to handle different levels of risk, depending upon various factors such as:

- The magnitude and type of the TPSP services provided (e.g., single contractor, cloud provider, etc.)
- The volume of exposure to a CHD or CDE compromise
- The probability and frequency of threats to the organization or its assets
- Whether the TPSP has ever been involved in a compromise of cardholder data

The *PCI DSS Risk Assessment Guidelines* provide further information for conducting a risk assessment and can be referenced by entities looking for more detailed guidance in this process.

Below is a high-level list of some of the questions and topics that may be appropriate to consider as part of the risk assessment. The list is not exhaustive and is meant as a starting point for an organization to use when creating its own risk-assessment process:

Security Governance and Risk Management

- Does the TPSP have an information security program in place that includes documented policies and procedures?
- What types of internal or external audits, if any, are performed at the TPSP's location(s)?
- Are there other PCI or other industry standards that are applicable to the environment or TPSP?
- Does the TPSP conduct periodic vulnerability scans and penetration tests on assets, applications, and systems containing customer data?
- Does the TPSP formally reassess and re-evaluate its information security threats and risks at regular intervals, based on the frequency of emerging threats to its systems and processes? Is the assessment process based on a standardized risk-assessment methodology (referenced in PCI DSS Requirement 12.2[7])?
- Has the TPSP ever had a data breach?

[7] This reference is to PCI DSS v3.1 – April 2015

Human Resources Practices

- How are background checks performed on resources that may have access to TPSP customer information? Are the background checks repeated at predetermined intervals?
- How are terminations handled?
- Are non-disclosure policies in place to protect both the TPSP and its customer information from disclosure?
- Does the TPSP have policies concerning transmitting, storing, and processing of sensitive data, as well as customer data?

Physical Security

- Is there a physical security program in place at the TPSP locations where applicable systems or services are provided?

Third-Party External Entities

- Do any external entities engaged by the TPSP have access to the TPSP's data processing facilities, systems, or applications?
- Does the TPSP perform due diligence on external entities with which it engages?
- Does the TPSP monitor the compliance and risk of external entities with which it engages?

Configuration Management

- Is there a formal change control and configuration management process in place at the TPSP?
- Does the TPSP update critical patches within a specified timeframe? Does it have a policy concerning patch management?
- Does the TPSP have any hardware or software that is no longer supported by the manufacturer (beyond its end-of-life)?
    - Are systems and applications hardened according to a documented standard?
    - Does the TPSP have secure configuration baselines for all of the platforms comprising its common service infrastructure?

Access Authorization

- How is logical and physical access to customer data and assets authorized?
    - If systems-access processes are shared, are the roles and responsibilities clearly documented?
- How are rights for physical and logical access reviewed?
- Does the TPSP always use a unique authentication credential (such as a password/phrase) for each customer?

Incident Response

- Does the TPSP have an incident response plan?
- Does the TPSP have procedures for reporting logical and physical security, and privacy incidents to customers?
- Do the TPSP procedures include contact information for authorities or forensic investigators?

Malware Controls

- What controls does the TPSP have in place to detect, contain, and eradicate viruses, worms, spyware, and malicious code?
- Are these controls implemented on all TPSP assets that transmit, store, or process the entity's cardholder data?
- What types of change-detection mechanisms are present on the TPSP's systems?
- Has the TPSP invested in any security products or services other than those required by PCI (anti-virus, FIM) that improve its ability to detect malware?

Segregation and Security Controls

- What controls are in place to keep customer systems, applications, and data segregated from other customer assets and inaccessible to other customers or the TPSP's internal network?

3.4 Documenting Results

An organization should also consider fully documenting the results of its research regarding the TPSP and review of the TPSP's compliance status. In addition to any other information and materials deemed necessary or appropriate through the due diligence process, each entity should strongly consider capturing and including the following pieces of critical data, as each will be invaluable in the future:

- Anniversary date – What is the date on which compliance documentation expires, requiring revalidation to have taken place?
- Compliance validation vendors – With what security and compliance vendors and assessors does the TPSP work? This may include QSAs, ASVs performing scans, etc.
- Acquiring bank – If applicable, with what acquiring bank does the TPSP work?
- Sponsor bank – Identify if the TPSP uses a sponsor bank for access to the payment card networks.
- Area audited – What specific service areas have been validated and how do they align with the services being provided to the entity?
- Nested service providers – Are there other TPSPs nested within the TPSP's compliance? What services do the nested TPSPs provide?
- Documentation of a shared responsibility model – The assessed entity should clearly document the PCI DSS requirements that are managed by each TPSP and those that are managed by the entity.

4 Engaging the Third-Party Service Provider

After successfully researching a TPSP and completing due diligence, the entity will seek to engage the TPSP. The following sections describe the important steps to consider when engaging a TPSP.

4.1 Non-Disclosure Agreement (NDA)

An NDA with TPSPs may be practical for your organization in the pre-selection process, and before any information is shared or disclosed. NDAs at this stage should be simple and concise, and should specify the purpose and the terms of the engagement. To simplify this process, it is recommended to have NDAs prepared by your legal department (or the party who takes care of your legal matters) prior to engaging any TPSPs, and make sure that your legal department is available to review any proposed changes or to review the TPSP's NDA document.

4.2 Set Expectations

As with any project, setting the expectations of all parties involved leads to a higher chance of success. Setting expectations is critical to achieve a consistent and agreed-upon mode of operation.

In addition to the other matters determined to be important by the parties, it is important to define, agree upon, and document each of the following expectations at the start of the engagement, and to review these expectations—at a minimum, annually and after a change in services—to ensure consensus is still maintained.

- The entity's fundamental goal is to clearly understand the TPSP's PCI DSS compliance status and as a result, enable itself to achieve and maintain its own PCI DSS compliance and gain assurance that the TPSP is sufficiently safeguarding the entity's CHD in the TPSP's possession.
- TPSP responsibility to sufficiently safeguard the entity's CHD in its possession, in an agreed-upon manner.
- The specific services provided by the TPSP to the entity.
- The primary points of contact at both the entity and the TPSP. In this regard, it may be important to identify specific individuals, along with back-up personnel in case the primary point of contact (POC) is not available. Contact information including e-mail, office phone, and cell phone are also important to document. These (or other specified) individuals should be held accountable for the due diligence activities, in addition to assuming communication responsibilities, addressing incidents, and providing compliance-related information.
- The entity may want to consider including in its review of and potential contract with the TPSP that the TPSP maintain the appropriate level of expertise in security and compliance relative to the service(s) they are providing to the entity. This can be especially critical for higher-risk TPSPs.

4.3 Gain Transparency

Correctly assessing the scope of the TPSP's responsibility in safeguarding the entity's CHD or CDE is critical, as the opinions of individuals and organizations regarding scope may differ. In order for this to occur, the entity may wish to consider requesting to view evidence proving the scope is accurate based upon what the TPSP has claimed. As detailed in section 3.2.2, "Third-Party Service Provider Validation Documentation," this information may be proprietary or confidential and may require redaction, remote viewing, in-person viewing, or phone discussions. Ideally, an ISA or a QSA should review the evidence provided to verify the scope is indeed applicable, appropriate, and accurate. An individual who is well-versed and experienced in network design and segmentation may also provide this expertise if an ISA or QSA is not available.

Entities may also wish to consider the use of appropriate contractual provisions with TPSPs that enable and require appropriate evidence sharing, to avoid situations where the TPSP is not obligated to facilitate the evidence-sharing process. If all attempts fail to gain required evidence from the TPSP, the entity may consider requesting that the TPSP document its scope definition in writing and include a provision for the TPSP to retain the documentation for the agreed-upon duration. Additional information can be found in Section 5, "Written Agreements, Policies, and Procedures."

4.4 Establish Communications

One of the keys to the success of the entity–TPSP relationship is effective communication. Without effective communication, changes may be made by the TPSP without the entity's awareness or agreement that may negatively impact the entity's overall PCI DSS compliance status. Determination of a significant change will vary from entity to entity, depending on the type of change and its impact.

Communications may be promoted and enhanced by establishing communication schedule as part of the onboarding process for the monitoring program, assigning the primary points of contact at the entity and the TPSP as the responsible parties for proactively communicating on important matters. If appropriate, these points of contact may also be responsible for distributing the information appropriately within the relevant organizations in a timely manner so that risk may be mitigated.

The communication schedule should be reviewed and updated on an annual basis or as needed, depending on the type and impact of changes. The following topics (non-exhaustive list) may need to be communicated whenever changes occur and/or annually, as applicable.

- Changes to the CDE
- Changes to the entity's or TPSP's payment processing structure
- Changes in personnel responsible for maintaining operations with the TPSP and entity
- Changes in personnel involved with the due diligence initiative
- Changes in processes, procedures, and methodologies that impact the CDE
- All other instances where an activity will impact the scope of the entity

4.5 Request Evidence

In addition to the evidence requested to support the services and scoping provided by the TPSP, the entity may need to verify that appropriate procedures were followed and controls deployed to support changes. To that end, the entity may determine that it is appropriate to request supporting evidence whenever it receives a communication from the TPSP and assesses the risk to be applicable. See Section 4.3 "Gain Transparency," above for applicable materials and methods of communication.

If the entity itself will assess the PCI DSS compliance status of the TPSP—i.e., the entity will employ the services of one of its own ISAs or an external QSA to determine the TPSP's compliance—requesting evidence annually may be appropriate to support the PCI DSS assessment.

4.6 Obtain Information about PCI DSS Compliance

Section 3.2.2, "Third-Party Service Provider Validation Documentation," provides examples of the information that may be obtained from a TPSP regarding its compliance status, whether the TPSP has been validated or is not required to validate. It is an option for entities to perform a PCI DSS compliance assessment of the applicable services provided by the TPSP by either employing the services of one of its own ISAs or an external QSA. This PCI DSS assessment should ideally be performed upon the start of the engagement. However, performing the assessment after the engagement has begun can still provide insight and a baseline to work from; and then annual assessments may be performed preferably ending a few months before the entity's own PCI DSS assessment date to allow for any remediation necessary.

As with the pitfalls detailed in Section 4.3, "Gain Transparency," above, the effectiveness of performing this type of assessment depends on the TPSP's willingness to provide the necessary information. Depending on the legal agreements between the parties, there may be many instances where the TPSP declines to provide proprietary and confidential information. As detailed in "Gain Transparency," the entity may wish to request that the TPSP document its refusal to provide the information in writing, if appropriate.

4.7 Frequency of Review

The following table shows the suggested frequency of review for the engagement steps:

Engaging Third-party Service Providers			
Steps	**Initially**	**As Changes Occur***	**Annually**
▪ Set Expectations	**X**	**X**	**X**
▪ Gain Transparency	**X**	**X**	**X**
▪ Establish Communications	**X**	**X**	**X**
▪ Request Evidence	**X**	**X**	**X**
▪ Obtain Information about PCI DSS Compliance	**X**		**X**

* ***Note:*** *Depending on the type of change introduced, this step may or may not be required. For example, a significant infrastructure change may initiate all steps, whereas a change that does not impact the CDE or PCI DSS compliance—for example, changes in primary point of contact—may only trigger a few steps. The result of risk assessments performed during the due diligence process will help determine how often these steps need to be repeated.*

4.8 Mapping of Third-Party Services to Applicable PCI DSS Requirements

It is critical that the entity fully understands how the services and products provided by the TPSP map to the PCI DSS requirements, so the entity can determine the security impact to its cardholder data environment.

The requirements that are applicable to a TPSP will vary depending on a number of factors, including the nature of services provided, the level of access it has to CDE, and so on. For example, a TPSP that provides firewall management services may have to meet PCI DSS Requirement 1[8]; a TPSP providing maintenance services that include incidental access to the CDE may require background checks and/or escorts while in sensitive areas.

Appendix A to this document provides a table showing suggestions and discussion points that may help clarify and determine how responsibilities for maintaining PCI DSS requirements may be shared between the entity and the TPSP. **Appendix B** is a sample PCI DSS Responsibility Matrix to help an entity start building an understanding of how PCI DSS requirements could map to the services that an entity outsources to a TPSP and the related accountability for each.

[8] This reference is to PCI DSS v3.1 – April 2015

5 Written Agreements, Policies, and Procedures

Note: *The information and guidance provided in this section and generally throughout this Information Supplement do not constitute legal advice and, accordingly, should not be relied upon or construed as such. Entities seeking to engage a TPSP to perform services are strongly encouraged to seek legal advice from an appropriately qualified professional to ensure that each party fully understands its rights and obligations, and that the parties' expectations are in alignment. Entities with specific questions about legal matters should consult an appropriately qualified legal professional. The information and guidance provided in this section do not supersede local or regional laws, government regulations, or other legal requirements. Ultimately, the specific terms of the agreement between an entity and a TPSP should reflect all of the details of the services being provided and the relevant rights and responsibilities of both parties.*

Once an appropriate risk-assessment process has been completed and a TPSP has been selected for an engagement, best practice suggests that the entity and TPSP should document their agreement in writing. The discussion below is intended to highlight certain issues specific to a typical entity–TPSP relationship that an entity may want to consider when seeking to engage a TPSP. Entities with existing agreements with TPSPs may also wish to consider the following when reviewing those agreements. The following is not intended to be an exhaustive list and is provided as a convenience in order to help familiarize entities seeking TPSP engagements with the kinds of issues that commonly arise in this context. Other issues may arise and may be equally or more important, and entities are strongly encouraged to seek appropriately qualified legal counsel in connection with all business agreements.

5.1 Agreements between PCI DSS Compliant Third-Party Service Providers versus non-PCI DSS Compliant Third-Party Service Providers

TPSPs that have undergone PCI DSS compliance assessment and are validated as compliant:

When engaging a TPSP that claims its services are PCI DSS compliant, entities should consider documenting such compliance. The specific documentation that may be provided will ultimately depend on the situation and agreement between the parties, and may include provision of an AOC, SAQ, and/or relevant sections from the ROC (redacted to protect any confidential information), including:

- Date of compliance assessment
- System components, services, and environments that were included in the third-party PCI DSS assessment
- System components and services that were excluded from the PCI DSS assessment, as applicable to the service(s) provided

Having the TPSP resources available (including ISA or QSA if required) to answer any clarification questions may be useful in validating that the services provided by the TPSP are covered. Similarly, provisions acknowledging the respective responsibilities of the parties for handling and securing the CHD in their possession in a PCI DSS compliant manner may assist in validation. Tracking the frequency of the

compliance validation may also assist in managing and monitoring the TPSP as required by PCI DSS Requirement 12.8[9].

TPSPs that have not undergone an assessment or are not required to validate PCI DSS compliance:

An entity that is required to establish PCI DSS compliance and that utilize the services of a TPSP that has not affirmatively established its own PCI DSS compliance may need to cover some or all of the TPSP's environment as a part of its own PCI DSS assessments. More specifically, such an entity's PCI DSS assessment will need to cover any TPSP service that requires (or may enable or permit) the TPSP to handle CHD or can impact the security of the CDE. As a result, entities seeking to engage TPSPs in this context may wish to consider mechanisms (such as the ability to audit the TPSP) intended to help promote transparency and assist in the PCI DSS compliance validation process, such as:

- Access to systems, facilities, and appropriate personnel for on-site reviews, interviews, physical walk-throughs, etc.
- Review of TPSP policies, procedures, process documentation, configuration standards, training records, incident response plans, etc. that evidence satisfaction of applicable PCI DSS requirements and/or requirements that the TPSP adhere to the entity's policy.
- Review of evidence (such as configurations, screen shots, process reviews, etc.) to assist in validating that all applicable PCI DSS requirements are being met for the in-scope system components of the TPSP environment.
- Clarity regarding portions of the merchant environment managed by the TPSP that are in scope for the entity/merchant PCI DSS assessment.
- Retention of evidence collected because of non-compliance
- Allocation of responsibility for handling and securing cardholder data in a PCI DSS compliant manner.
- Frequency of PCI DSS compliance validation/assessment (e.g., annually, quarterly, etc.).

5.2 Considerations when Building Agreements, Policies, and Procedures

Regional Regulatory Requirements

It is recommended that an entity evaluate all regional (e.g., country, state, provincial, municipal) requirements that may apply. For example, some merchants, such as state agencies or public universities, may be required to comply with state-specific requirements regarding specific issues (such as budget-cycle dependence for payment) or selection of a TPSP. An entity should consult appropriate federal, regional, state (e.g., state controller), local, and foreign agencies to determine applicable limitations and guidelines.

[9] This reference is to PCI DSS v3.1 – April 2015

Legislative Considerations

An entity may want to consult applicable laws that may contain additional provisions regarding:

- Definitions of sensitive or protected information
- Breach-notification thresholds
- Specific identity-theft protection requirements
- Enhanced protection requirements for specific categories of sensitive or other data

These provisions may vary from an entity's typical policy or agreement. The entity should seek legal consultation regarding all applicable legal, regulatory, and other requirements for each jurisdiction, area, and region in which it will be operating. The value of understanding and allocating responsibility for meeting all such requirements cannot be understated, especially in the location(s) where physical and virtual payment environments reside.

Acquirer Considerations

Each acquirer may have its own requirements related to engaging a TPSP. An entity may want to review its agreements with acquirers to ensure its TPSPs (or the acquirers' TPSP(s)) are meeting any additional acquirer-specific responsibilities that flow through to TPSPs.

Payment Card Brand Considerations

Each payment card brand has created its own compliance programs. Entities seeking to engage TPSPs should consider reviewing these compliance-program requirements with the TPSP(s) in order to identify and appropriately allocate corresponding responsibilities, and to ensure that each understands and complies with all applicable payment card brand mandates.

Industry-Specific Considerations

In various industries and verticals there are specific industry regulations and requirements that entities might consider, as they may be important to the relationship and the allocation of rights and responsibilities between an entity and a TPSP. Specific issues to consider may include the handling of equipment that is part of the CDE, data-destruction requirements, and levels of protection required to meet compliance requirements. An entity and TPSP should discuss any industry-specific requirements that may be pertinent.

Internal Policy-Specific (Subsidiary Relationships) Considerations

In the event that a parent company and its subsidiary establish a relationship where one is a TPSP and the other is utilizing the TPSP services, additional issues to consider may include:

- Is the TPSP incorporating subsidiaries into its PCI DSS assessment or performing separate PCI DSS assessments among those subsidiaries?
- Is the TPSP considered a different level merchant/service provider than the entity? Does that affect the type of validation that either of them must perform?

- What does the TPSP actually provide to the entity?
- What other aspects of the relationships may be relevant (e.g., independent franchisee vs. corporate franchisee)?

Note: *There is a high degree of variability in the formality of contractual arrangements between parent and subsidiary companies. Such arrangements range from unwritten agreements, to informal internal service-level agreements, to sophisticated arm's length contracts. Nonetheless, the issues and concerns likely to arise between unrelated entities and TPSPs are also likely in the parent-subsidiary context.*

5.3 Additional Considerations

Entities seeking to engage TPSPs may also wish to consider the following.

5.3.1 Responsibility Matrix

A responsibility matrix is typically a schedule or appendix that details specific responsibilities of the parties to an agreement, in an easy-to-understand, tabular format. A responsibility matrix in the entity–TPSP context may be useful in helping to identify a variety of issues, including but not limited to responsibilities, procedures, and notice periods for the following:

Technology

- Purchasing of system components
- Building of system components
- Testing/Deployment
- Sustainment/maintenance (i.e., patching, vulnerability, and penetration testing)
- Product or technology life cycle

Processes

- Operational procedures
- Notification requirements
- Superseding policy (in the event of a discrepancy, which policy will be considered valid)
- Reporting
- Audit procedures that include systems and facilities as required
- PCI DSS validation activities
- Access to systems/data for periodic validation if required (account reconciliation, logs, etc.)
- Access to systems/data for forensic investigation
- Data/evidence retention and destruction
- Business recovery and continuity

Furthermore, it may be appropriate (though not required by PCI DSS) to define the responsibilities on a per-requirement basis. See Appendix B for an example.

5.3.2 Data Breaches

As outlined in PCI DSS Requirement 12.10[10] regarding the incident response plan, numerous specific actions may be required in connection with suspected data breaches, within a very short time of such breach. Entities may wish to consider how best to ensure that the TPSP is aware of these requirements and develop a workflow establishing when, how, and who a TPSP must notify in case of a suspected data breach. In addition to the incident response plan required by PCI DSS, payment card brands and national or regional laws may require breach notification. Entities should consider each of these issues with relevant TPSPs, and how best to allocate responsibility for all applicable notification requirements and all requisite follow up actions. Entities are also strongly encouraged to include in their contract with TPSPs that in the event of a breach/compromise, the TPSP must participate fully with a PCI forensic investigator (PFI) and the forensics investigation, including making the entity's data, systems, components, and related services available for investigation.

Additional considerations may include issues such as:

- Steps expected of entities and/or TPSPs if data loss has occurred
- Use of tools such as file recovery
- Applicability and adequacy of insurance coverage
- Responsibility for making notifications
- Financial responsibility for notification costs
- Notification timelines
- Engagement of forensic investigators and responsibility for investigation costs
- Clearly documenting the incident (involving cardholder data) response reporting requirements, including who is responsible for notifying the acquirer or card brands in case of a third-party incident

5.3.3 Post-termination Considerations Regarding TPSPs and their Customers

Entities that (a) are subject to requirements regarding CHD or any CDE (whether driven by the PCI DSS, legal considerations, or otherwise) and (b) outsource related responsibilities to a TPSP, may also wish to consider how those requirements and responsibilities may apply to the TPSP **after** the entity–TPSP engagement has formally ended. For example, if a TPSP continues to store an entity's CHD as part of an archival backup system, the TPSP's corresponding obligations regarding such CHD may continue as well. As a result, the entity may wish to consider whether post-termination reporting, notice, data retention, or related requirements are appropriate and/or whether notice should be provided (even after the entity–TPSP relationship has ended) if and when the TPSP destroys or irreversibly removes data from its facilities and/or devices.

Similar considerations arise in connection with terminated TPSP employees. If an individual may have access to the entity's confidential information (including CHD or the CDE) while employed by the TPSP,

[10] This reference is to PCI DSS v3.1 – April 2015

entities and TPSPs may wish to consider mechanisms to help ensure that such information is protected after the employment relationship ceases, such as:

- Ongoing post-termination confidentiality obligations
- Appropriate allocation of responsibility for ensuring compliance by TPSP employees with their ongoing confidentiality obligations
- Appropriate allocation of responsibility for enforcement of confidentiality obligations, and for costs associated with enforcement and related legal proceeding in the event of a breach of those obligations
- Termination of TPSP-employee access to buildings or systems immediately upon termination of employment

5.3.4 Outsourcing of Provided Functionality (Nested TPSPs)

If the TPSP outsources to a separate contractor a portion of the services the TPSP has agreed to provide to the entity, all of the issues and concerns raised above would potentially also apply to the relationship between the TPSP and the outsourced contractor. This, in turn, may impact the scope of the entity's CDE and ultimately the scope of the entity's PCI DSS validation. As a result, to help manage these complexities and related risks, entities may wish to consider whether mechanisms such as the following may be appropriate:

- Notification to the entity that outsourcing has occurred
  - The TPSP that has been initially engaged to provide services to the entity seeking PCI compliance should provide as part of the initial engagement documentation with information related to other third-party entities (for example, nested TPSPs) that will be engaged in supporting the entity.
- Appropriate limitations regarding outsourcing of functionality, such as regional exclusions due to jurisdictional concerns
  - The entity seeking a TPSP for outsourcing of services that could impact the security of the cardholder data environment should establish documented procedures for the inclusion of clauses with detailed limitations and exclusions depending on the type of services to be outsourced and jurisdictional and regulatory compliance concerns (e.g., country-level data privacy laws, safe-harbor rulings, etc.), avoiding general liability statements and focusing more on the uniqueness of the inherent risks associated with the services to be outsourced.
- Appropriate allocation of liability, responsibility and costs relating to actions of outsourced contractors and/or notifying the entity regarding incidents

While an entity's obligation to satisfy Requirement 12.8.4[11] extends only to monitoring and collecting evidence of the compliance status of its directly contracted TPSPs, the entity may also want to carefully review its TPSPs' reliance on, and continuous oversight of, any nested TPSPs.

[11] This reference is to PCI DSS v3.1 – April 2015

5.3.5 Loss of Compliance Status

Loss of a TPSP's PCI DSS compliance status can have significant ramifications for an entity relying on the TPSP's services. Accordingly, entities may wish to consider mechanisms intended to keep the entity apprised of changes in PCI DSS compliance status, and to appropriately allocate responsibility for loss of compliance status among the parties. Such mechanisms may include:

- Disclosure/notice of changes in compliance status to the impacted entity
- Remediation plans and procedures to re-establish compliance by set dates
- Regular status meetings to advise on remediation efforts
- Other appropriate measures intended to help ensure accountability and responsibility for non-compliance

6 Maintaining Relationships with and Monitoring Third-Party Service Providers

Establishing and maintaining a program to monitor TPSP compliance with PCI DSS Requirement 12.8.4[12] is a critical requirement for any entity. A monitoring program will allow an entity to monitor the compliance status of TPSP(s) and determine whether a change in status requires a change in the relationship. Validation of compliance takes place at a single point in time, and unfortunately it is quite easy for an entity to allow processes to relax and for compliance to lapse. Relying on other parties for services—including outsourcing critical functions—does not relieve an entity of responsibility for the security of its cardholder data, and TPSP compliance must be monitored continuously and diligently.

Investing the time and effort to develop and implement a strong TPSP monitoring program provides numerous benefits to the entity. First, and most importantly, the monitoring program will improve the entity's security posture and help ensure the protection of cardholder data for which the organization is responsible by providing assurance and awareness about whether the TPSP continues to share the same level of commitment in handling CHD. A monitoring program will also ensure there is regular communication between the TPSP and the entity regarding changes to the environment including processes and procedures. This allows the entity to be in a proactive—instead of reactive—position. Second, the monitoring program will provide a consistent process to simplify the ongoing monitoring and management of TPSPs. Finally, the monitoring program will enable an entity to demonstrate compliance with a key section of the PCI DSS, should proof be requested from a party performing an assessment.

As part of an entity's monitoring program, an onboarding process for new TPSPs should be developed and maintained, including providing new TPSPs with information attained through the various stages of engagement (i.e., risk analysis, contract details, responsibility matrix, etc.) This additional information should be incorporated into the monitoring program to create the framework for monitoring a TPSP.

6.1 Developing a Third-party Service Provider Monitoring Program

A TPSP monitoring program should be fully documented. This ensures there is a common understanding of its elements across the organization, facilitates delegating portions of the process if required, and allows review of the process by outside parties when necessary. The elements of the program should include processes, policies, and procedures, and assignment of responsibility for those elements to specific people within the organization. The program documentation should be revisited on a regular basis in order to make corrections and improvements as the business processes and TPSP relationships evolve. It is recommended that program documentation be reviewed at least on an annual basis and is approved by management.

The program documentation should cover the following areas, including guidance on the intent and importance:

[12] This reference is to PCI DSS v3.1 – April 2015

6.1.1 Cardholder Data Environment (CDE) Scope Definition

Ensuring the CDE scope is correctly defined and verified is pivotal in determining the level of effort required to achieve compliance. The entity needs to ensure that all resources involved in the monitoring of TPSPs understand the concept of CDE scope, and specify what is needed in order to fully define scope (e.g., a high-level network diagram with applications and network components clearly labeled, out-of-scope validation activities, etc.). Once scope has been confirmed, the program should include a deliverable that explains the CDE scope and indicates the role of each TPSP and how it impacts the entity's PCI DSS scope.

6.1.2 Maintaining an Inventory of Third-Party Service Providers

Define the procedures to maintain an inventory of all TPSPs, including the information elements deemed critical. The following are suggested elements that may be included in the inventory:

- Name and primary points of contact at the TPSP
- Specific service(s) being provided
- If cardholder data is shared, what elements are shared (sensitive authentication data, PAN, expiry, etc.)
- Location of the data—is the data stored internally in the organization, by the third party in one of its locations, or by an external hosting provider
- What system components are included in the review
- TPSP risk-assessment results
- Frequency of monitoring cycle
- Last date of review
- Contract renewal/expiry
- Documentation/evidence required
- Any nested TPSPs leveraged to provide the services
- Any third-party payment applications used to provide the services
- Volume of cardholder data that is stored/processed/transmitted/impacted by the TPSP
- Logical access to the entity's network
- Any designations the TPSP holds that support its PCI DSS compliance attestation (ISO, PCI QIR, PCI PTS, FIPS 140, etc.)

6.1.3 Third-party Service Provider Monitoring Procedure

Below is a high-level description of the components an entity may wish to consider including in its TPSP monitoring procedure. The list is not exhaustive and is not intended to define the only method to monitor TPSPs' PCI DSS compliance status; however, the list describes some recommended components that may be included in the procedure.

6.1.3.1 Documentation/Evidence

Define the evidence and supporting documentation that will be collected from TPSPs for analysis and retention. As specified earlier, a key piece of information to be gathered is the role of the TPSP in the CDE. This information may be available from the applicable sections of the ROC or Part 2E, Description of Environment in the AOC. See Section 3.2.2, "Third-Party Service Provider Validation Documentation," for additional information.

6.1.3.2 Third-party Service Provider PCI DSS Compliance Status Review

Describe the PCI DSS compliance status review process in detail, including specific information elements to be examined. In particular, it is important that reviewers compare the processes audited as part of the TPSP's assessment to the services provided to the organization. Describe any risks inherent in using services that were not included in the assessment. Develop a checklist to aid the reviewer. If possible, these criteria should be discussed and revised on an annual basis if the level or type of service changes.

6.1.3.3 Results Write-up

Develop a report specification—or even a reporting template—to aid the reviewer in documenting the results of the review of the TPSP PCI DSS compliance status. Documentation should be done in a very consistent manner so that, as different reviewers in the organization participate in the process, they generate similar deliverables. The write-up may include the anniversary date, compliance validation vendors, acquiring bank, sponsor bank, and areas audited.

6.1.3.4 Review Follow-up

Specify how TPSP PCI DSS compliance status review results are to be shared and approved internally. Determine steps and timelines for sharing results with the reviewed TPSP, and set expectations with the TPSP if additional work is needed. Describe the escalation procedures that should be carried out if a TPSP falls into a non-compliant status or refuses to obtain or prove PCI DSS compliance or is not required to validate PCI DSS compliance.

6.1.3.5 Access Control and Data Retention

Define policies for monitoring and control of program deliverables (for example, supporting documentation, evidence, and results reporting) during generation and subsequent storage. Set a specific policy for retention of monitoring-program data; it is recommended that documentation be retained for a minimum of a rolling three (3) year period.

6.2 Other Considerations

Note: *The following section may be used as a guide on suggestions of how to proceed with a particular scenario. These actions can have unforeseen consequences and should be thoroughly reviewed for impact and risk before engaging in any of the suggested activities.*

6.2.1 Third-party Service Provider Does Not Provide Requested Information

If a TPSP is unresponsive, or is unable or unwilling to provide the information requested, consider the following actions:

- Ensure all communication attempts are documented
- Attempt to obtain an explanation from the TPSP: Is too much information being requested?

  Note: *The AOC and/or the relevant sections of the ROC may be sufficient to demonstrate the scope of the assessment and verify its compliance status. Another option to verify the TPSP's compliance status may be to view the documentation either at the TPSP location or remotely, over a secure session.*

- If the TPSP has an acquiring bank, contact that bank and request assistance with the TPSP to produce the necessary information.
- If all attempts to obtain the requested data have failed, it may be appropriate to involve the payment card brands.
- If PCI DSS submission requirements are documented in the contract or agreement with the TPSP, notify the TPSP that the agreement terms are being enforced.
- If all else fails, note in the relevant sections of the ROC under Section 4.8[13], "Service providers and other third parties with which the entity shares cardholder data," the services provided by the TPSP could not be verified due to non-communication and non-cooperation.
- Note the challenges of the TPSP in the monitoring program documentation and increase the risk level of the TPSP until the next review cycle.

6.2.2 Third-party Service Provider has not Validated PCI DSS Compliance

If a TPSP is not advancing its PCI DSS compliance, has allowed its compliance to lapse, does not intend to validate, or is not required to validate PCI DSS compliance, consider the following actions:

- Talk to the TPSP to determine the gap in compliance (e.g., which PCI DSS requirements were not met, which systems and/or processes were not compliant, which services have not been validated, etc.).
- Request evidence from the TPSP to show the applicable PCI DSS requirements are being met for the required services as detailed in Section 3.2.2, "Third-Party Service Provider Validation Documentation" related to TPSPs that have not validated PCI DSS compliance.

[13] Refers to revision 1.0 – April 2015

- If TPSP has undergone an assessment and has submitted documentation for PCI DSS validation to the payment card brands and the list(s) have not yet been updated, request a copy of the evidence submitted to verify the applicable PCI DSS requirements are being met for the services provided.
- If required, notify the entity's acquiring bank of the situation and discuss whether the acquirer has specific steps to mitigate risk (e.g., action plan, remediation activities).
- If the TPSP has not yet completed PCI DSS compliance, ask for a detailed plan with deadlines for finalizing the PCI DSS compliance process; make sure the TPSP provides status checks on a regular frequency until it achieves PCI DSS compliance.
- Discuss with the TPSP the frequency for checking into its PCI DSS compliance activities, recommended 30-60 days prior, to the annual PCI DSS assessment deadline.
- Ensure future agreements with TPSPs are developed with the guidelines within this document in mind, and understand the organization's positions and requirements related to PCI DSS compliance as new TPSP candidates are interviewed.
- Notify the TPSP of any requirement for a notice period for any changes to the service or support of the service, to allow time for a risk assessment to determine whether the change will impact PCI DSS compliance or applicable PCI DSS requirements.
- Notify any TPSP that is not required to validate PCI DSS compliance that changes in PCI DSS requirements, payment card brand mandates, or critical changes that alter the relationship with the TPSP may result in a requirement for the TPSP to validate PCI DSS compliance.
- If evidence cannot be obtained from the TPSP to verify that the applicable PCI DSS requirements are being met, the TPSP environment and system components that provide the services for the entity may need to be reviewed as part of the entity's annual PCI DSS assessment review, and may be subject to remediation effort to meet PCI DSS compliance. Note in the relevant sections of the ROC under Section 4.8[14], "Service providers and other third parties with which the entity shares cardholder data," and with the applicable PCI DSS requirement, the TPSP services that are part of the assessment.
- Note the challenges of the TPSP in the monitoring program documentation and consider any corresponding change in the risk level assigned to the TPSP until the next review cycle.
- If PCI DSS validation requirements are documented in the contract or agreement with the TPSP, notify the TPSP that the agreement terms are being enforced.

6.2.3 Third-party Service Provider Validates PCI DSS Compliance via Inclusion within the Entity's PCI DSS Assessment

A TPSP's service can be included within the scope of the entity's CDE. The following are considerations for inclusion:

- Confirm that this situation is acceptable to the acquirer and/or payment card brand.

[14] Refers to revision 1.0 – April 2015

- Identify systems and process to be included within the entity's PCI DSS assessment.
- Ensure that the TPSP is advised of any expectations of improvements to the service and its, sustainability.
- Notify the TPSP of any requirement for a notice period for any changes to the service or support of the service – to allow an assessment to determine whether it will impact on compliance.
- The TPSP will need to be made aware of and understand that as it is now included as part of the entity's compliance assessment, business changes of the TPSP could adversely impact the compliance status of the entity.
- Clearly define "right to audit" requirements including timeframes and who is responsible for cost incurrences if the merchant will be assessing the TPSP instead of relying on an AOC or other form of compliance evidence from the third party.

6.2.4 Existing or New Service or Process is not PCI DSS Compliant or will make the Entity or TPSP non-PCI DSS Compliant

It is critical to maintain awareness within the payment card industry that there are various non-compliant entities working at becoming PCI DSS compliant and that these entities will attain their own compliance at different times, depending on the complexity of the respective CDE. The difference in compliance status can create a situation where a PCI DSS compliant entity or TPSP is contracted to a non-compliant entity or TPSP that is actively working towards PCI DSS compliance.

If there is a shared non-compliant process or service previously not addressed, it would be appropriate for the agreements between the entity and the TPSP to detail whether the entity or TPSP is responsible for the applicable PCI DSS requirements. However, there is the possibility in previous PCI DSS audits this non-compliant status was not known, unintentionally not disclosed, or not fully understood, which may lead to an existing or new service to be found to be non-compliant.

If a requested service will cause the TPSP or entity to become non-PCI DSS compliant or if during provision of the service a situation arises that changes the attributes of the service, determination of the impact to PCI DSS compliance for both the entity and the TPSP may be appropriate. Examples of such scenarios could include an entity sending sensitive authentication data to its TPSP for storage, or a TPSP implementing an infrastructure change that impacts segmentation controls between its hosted entities' environments. It is recommended the following actions be considered:

- If an agreement is not currently in place between the entity and the TPSP—e.g., new service request, new TPSP relationship—it is recommended the entity and TPSP consider performing an additional risk assessment to determine whether and how to proceed.
- If an agreement exists between the entity and the TPSP, the entity may consider an examination of the contract or agreement with the TPSP to determine which party is responsible for mitigating the non-compliant data or process.
    - Consider whether the non-compliant service or process is essential and the impact of stopping it as soon as possible until a solution can be developed.

- For business-critical issues, the entity and TPSP should work together to determine who will be accountable for the cost and responsibility for correcting the issue, if necessary. Discuss with legal counsel to ensure the entity or the TPSP and any nested TPSP use appropriate agreement/contract change provisions or clauses to negotiate a fair and reasonable timeframe to remediate the non-compliance issue.
- Discuss with the TPSP and agree on introducing compensating controls as soon as possible that mitigate the risk of continuing with the non-compliant process or data exchange—while work continues on its remediation.
- Prepare a remediation plan that can be provided to the entity or the TPSP in a form that can be used as evidence (e.g., Compensating Controls Worksheet) to provide a QSA if a PCI DSS compliance review is due within the remediation timeframe.
- Ensure any nested TPSPs meet the agreed obligations with regard to remediating the non-compliant issue and keeps the TPSPs informed of progress.

Appendix A: High-Level Discussion Points for Determining Responsibility

These high-level suggestions and discussion points may help clarify how responsibilities for PCI DSS requirements may be shared between an entity and its TPSP(s). Entities should consider defining these responsibilities in written agreements with TPSPs. The table in this Appendix may also help in completing a detailed PCI DSS responsibility matrix (sample in **Appendix B**) and determining who will be responsible for each control area.

The table consists of the following fields:

- **Steps to Determine Responsibility:** High-level control areas that may cover multiple PCI DSS requirements and a starting point for discussion between the entity and its TPSP.
- **Discussion Points**: High-level discussion points for each control area. These recommendations are for discussion between the entity and the TPSP to assist in understanding the control areas and allocating the responsibilities in each.
- **Entity or Third Party:** These columns may be used to track responsibility for each control area for the services being provided, any discussion items that need follow-up, or whether the control area is a shared responsibility.
- **Evidence to be Provided**: This column may be used to document evidence to be provided per the mutual agreement by the TPSP and the entity to support the entity's validation in meeting the control area.

For the full PCI DSS and related documents, please see the PCI SSC website https://www.pcisecuritystandards.org/security_standards/documents.php.

Note: *This Appendix is intended as guidance only and is for optional use at the discretion of the entity and/or TPSP; completion of this Appendix is not a requirement. The allocation of responsibilities between an entity and its TPSP(s) ultimately will depend on the specific facts and circumstances and services provided. Although the items in this Appendix may be useful in helping to allocate responsibilities between an entity and its TPSPs, the list of items and discussion points in this Appendix is not exhaustive. Each organization seeking to engage a TPSP must determine what is relevant in light of the circumstances, the organization's payment environment, the proposed TPSP's role, and other factors determined to be important through thorough due diligence.*

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
System Components (e.g., Firewalls, Servers, Applications, Appliances)				

Determine the procedures for the design, staging, implementation, and ongoing maintenance of system components.	• Firewall Reviews
	• Encryption of transmissions over public networks and end user messaging systems
	• System updates and maintenance including
	  ○ Patching cycles
	  ○ Operating system vs. application
	  ○ Virtual vs. physical
	  ○ Centralized tools and reporting
	• Isolation strategies (segmentation, intrusion detection/prevention)
	• Change management procedures
	• Anti-virus deployment strategies
	• Change-detection strategy for critical files
	• Risk-based analysis including risk-assessment results
	• Access control procedures
	• Defining roles
	  ○ Approval process
	  ○ Entitlement reviews
	  ○ Revocation procedures
	  ○ Two-factor requirement
	  ○ ID and password requirements
	  ○ Session timeouts and login requirements
	  ○ Incident response
	• Time synchronization (Network Time Protocol)			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
Determine procedures for testing the implementation and ongoing maintenance of system components.	• Functional testing • Internal and external network vulnerability scans – frequency • Penetration testing (application and network level) • Rogue wireless detection • Detection of unauthorized wireless access points.			
Determine the documentation required to meet all applicable PCI DSS requirements.	• System configuration security basis • Network diagrams • Justification of ports, protocols, services, and daemons			
Determine resources and documentation necessary to assist with producing evidence and assist with validation.	• Develop RACI (Responsible, Accountable, Consulted, Informed) chart to determine resources necessary to assist with: o Daily operational procedures o Evidence gathering o Remediation assistance o Assessment participation – Implementation staff – Administrators – Support staff – Managers – Penetration testers – IT Security – Change management team – ASV – Incident response team			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
Stored cardholder data				
Determine retention periods for cardholder data (CHD) storage.	• Legal, regulatory, and business needs. • Justification of CHD storage			
Determine procedures for the secure disposal of CHD.	• Shredding, pulping of physical media • Secure wipe of electronic media			
Determine procedure for the verification of CHD that does exist or is transformed.	• Transformation technologies (tokenization, encryption, etc.) • Known locations where CHD is stored in all media types • Applications, business processes and physical/logical locations where masked CHD is displayed			
Determine the procedures for any transformation technologies.	• Types of cryptography in use • De-tokenization procedures if available or required • Key-management procedures including RACI chart			
Determine procedures to ensure that storage and transport of cardholder data—including physical media containing cardholder data—is done securely.	• Backup media storage security • Review frequency of storage-location security • Media distribution process • Media classification • Process for all media sent outside the facility • Frequency of media inventory enumeration			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided

Determine resources and documentation necessary to assist with:
• Producing evidence
• Validation
	• Develop RACI chart to determine resources necessary to assist with
	  ○ Daily operational procedures
	  ○ Evidence gathering
	  ○ Remediation assistance
	  ○ Assessment participation			

Develop and Maintain Secure Code				
Determine application software-development methodology and information security within the software-development lifecycle.	• Software-development processes basis (i.e., industry standards and/or best practices) • Code-reviews processes • Processes for training in secure coding techniques (e.g., OWASP) for developers (based on industry best practices and guidance)			
Determine RACI requirements for software-development lifecycle.	• Separation of duties between development/test and production environments • Production data (live PANs) used in testing or development • Remediation of vulnerability and penetration testing results/issues • Change management			

Determine resources and documentation necessary to assist with:
• Producing evidence
• Validation
	• Develop RACI chart to determine resources necessary to assist with:
	  ○ Daily operational procedures
	  ○ Evidence gathering
	  ○ Remediation assistance
	  ○ Assessment participation
	  – Developer resources
	  – User-acceptance testing (UAT) testers
	  – Quality assurance testers			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
Physical access				
Determine the procedures associated with physical security controls for each computer room, data center, and other physical areas with systems in the CDE.	• Facility entry controls for limiting and monitoring physical access to systems in the CDE			
Determine process and procedure for assigning badges to onsite personnel and visitors.	• Visitors • Onsite personnel			
Determine resources and documentation necessary to assist with: • Producing evidence • Validation.	• Develop RACI chart to determine resources necessary to assist with: ○ Daily operational procedures ○ Evidence gathering ○ Remediation assistance ○ Assessment participation			
Access to CDE and/or CHD				
Determine procedures associated with granting, managing, and monitoring user access to CHD or CDE.	• Types of access to CHD/CDE ○ Internal ○ External • Granting credentials • Revoking credentials • Roles and responsibilities • Limitations of access			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided

Determine procedures associated with granting, managing, and monitoring vendor access to CHD or CDE.	• Types of access to CHD/CDE
	  ○ Internal
	  ○ External
	• Granting credentials
	• Revoking credentials
	• Roles and responsibilities
	• Limitations of access			

Determine resources and documentation necessary to assist with:
• Producing evidence
• Validation
	• Develop RACI chart to determine resources necessary to assist with:
	  ○ Daily operational procedures
	  ○ Evidence gathering
	  ○ Remediation assistance
	• Assessment participation
	  ○ Granting access
	  ○ Revoking access
	  ○ Monitoring access			

Logging				

Determine the process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	• Central logging requirements
	• Types of logs available—must meet applicable PCI DSS requirements
	• Protection of log integrity
	• Frequency of log collection
	• Retention of logs
	• Review and alerting procedures
	  ○ Log harvesting
	  ○ Log parsing
	  ○ Alerting
	• Investigation assistance procedures
	• Access to the logging system			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
Determine resources and documentation necessary to assist with: • Producing evidence • Validation	• Develop RACI chart to determine resources necessary to assist with: ○ Daily operational procedures ○ Evidence gathering ○ Remediation assistance ○ Assessment participation			
Maintain a policy that addresses information security for all personnel				
Determine which corporate policies will be enforced for each engagement.	• Which policy will supersede the other if required • Which policy will be communicated to all staff • Addresses all applicable PCI DSS requirements			
Determine the process for the annual risk assessment.	• Risk-assessment documentation • Risk-assessment frequency ○ Annually ○ After significant changes			
Determine the plan to develop a formal security-awareness program to make all personnel aware of the importance of cardholder data security.	• Frequency of training ○ On-boarding ○ Annually • Staff acknowledgement			
Determine procedures for conducting background checks.	• Procedures should be comparable • Legal considerations			
Determine the process for creating PCI monitoring program.	• Compliance attestation • Terms of engagement			

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
Determine the plan to develop an incident response plan to be implemented in the event of system breach.	• Incident response roles, responsibilities, and communication strategies			
Determine resources and documentation necessary to assist with: • Producing evidence • Validation	• Develop RACI chart to determine resources necessary to assist with: ○ Applicable policies ○ Evidence gathering ○ Remediation assistance ○ Assessment participation			

Appendix B: Sample PCI DSS Responsibility Matrix

A PCI DSS responsibility matrix may help to clarify and confirm how responsibilities for maintaining PCI DSS requirements are shared between the entity and TPSP. The High-Level Discussion Points for Determining Responsibility in **Appendix A** may help in the completion of a detailed PCI DSS responsibility matrix.

Considerations for each PCI DSS requirement include:

- Does the TPSP perform/manage/maintain the required control?
- How is the control implemented, and what are the supporting processes—e.g., process for patch updates would include details of testing, scheduling, approvals, etc.?
- How and when will the TPSP provide ongoing assurance and/or evidence to the entity that controls are met—for example, periodic reports, real-time notifications, results of testing, etc.?

Note: This Appendix is intended for optional use at the discretion of the entity and/or TPSP; completion of this Appendix is not a requirement nor is it necessary for an entity or TPSP to complete this Appendix to meet PCI DSS Requirement 12.8.5[15].

PCI DSS Requirement	Responsibility			Specific coverage/ scope of entity responsibility	Specific coverage/ scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
	TPSP only	Entity only	Shared			
1.1 Establish and implement firewall and router configuration standards that include the following:	☐	☐	☐			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	☐	☐	☐			
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	☐	☐	☐			

[15] This reference is to PCI DSS v3.1 – April 2015

PCI DSS Requirement	Responsibility			Specific coverage/ scope of entity responsibility	Specific coverage/ scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
	TPSP only	Entity only	Shared			
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	☐	☐	☐			
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	☐	☐	☐			
1.1.5 Description of groups, roles, and responsibilities for logical management of network components	☐	☐	☐			
1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed including documentation of security features implemented for those protocols considered to be insecure. *Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.*	☐	☐	☐			
1.1.7 Requirement to review firewall and router rule sets at least every six months	☐	☐	☐			
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	☐	☐	☐			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	☐	☐	☐			
1.2.2 Secure and synchronize router configuration files.	☐	☐	☐			
…And so on.						

Acknowledgement

The PCI SSC would like to acknowledge the contribution of the Third-Party Security Assurance Special Interest Group in the preparation of this document. The members include representatives from the following organizations:

2-sec Ltd.
24 Solutions AB
403 Labs, LLC
7Safe
Accudata Systems
Accuvant, Inc.
Acumera, Inc.
Agio, LLC
AJB Software Design
Amazon.com
American Express
American Lebanese Syrian Associated Charities Inc. (ALSAC)
Anitian Corporation
ANXeBusiness Corp.
Aon Service Corp.
Assurant, Inc.
AT&T Consulting Solutions
atsec (Beijing) Information Technology Co., Ltd
Australia Post
Australian Payments Clearing Association (APCA)
Bank of America N.A.
Bank of New Zealand
Barclaycard
Barnes & Noble College Booksellers Inc.
Basefarm A/S
Baylor University
BB&T Corporation
Bell Canada
Bill2Pay, an Intuition Systems Inc Company
Bit9 Inc.
Board of Trustees of the University of Arkansas
BP Products of North America
Bridge Point Communications
BrightLine CPAs & Associates, Inc.
British Airways PLC
BT Plc
Canadian Tire Financial Services
Capita PLC
Chase Paymentech Solutions
CIPHER
Citigroup Inc.
City of Calgary
Civica UK Ltd
Coalfire Systems, Inc.
College Entrance Examination Board
Comcast Cable Communications
Compass IT Compliance, LLC
Compliance3
ComplyGuard Networks Inc.
Comsec
Control Case
Control Gap
ControlScan
Convergys Corporation
Credit Union Australia
Crowe Horwath LLP
CVS Caremark
Deli Management Inc.
Dell, Inc.
Deloitte & Touche LLP (USA)
Digital Defense, Inc.
DSW Inc.
ECS Security Ltd.
EFM Consulting Inc.
Elavon Merchant Services
Espion LTD
EVO Payments International
Experian Information Services
Experis Finance US LLC
Fidelity Information Services (FIS)
FireHost
Fiscal Systems, Inc.
Fiserv Solutions Inc.
Fishnet Security

Florida's Turnpike Enterprise
Foregenix
Foresight IT Consulting Pty Ltd.
Fortrex
G2 Web Services, LLC
G6 Hospitality LLC
Games Workshop Ltd
Gap Inc.
GE Money
Gemserv Limited
Global Payments Direct Inc.
Grant Thornton LLP
GTT Communications Inc.
GuidePoint Security, LLC
Heartland Payment Systems
Henry Ford Health System
Hitachi-Omron Terminal Solutions, Corp
HP Information Security UK Limited
HyTrust Inc.
IBM Corporation
Information Risk Management (IRM)
Inline Technologies
Integralis Ltd Europe
Interac Association
International Card Processing Services (ICPS) Ltd
Internet Security Auditors
IQ Information Quality
Kilrush Consultancy Ltd
KnowIT Secure AB
KPMG, LLP
La Maison Simons Inc.
Levi Strauss and Co
Limited Brands Inc.
Lloyds Banking Group
Lowe's Inc.
M4 Products and Services
Mako Networks Ltd
Market America Inc
Marsh and McLennan Companies (MMC)
MegaPath Inc.
MegaplanIT, LLC
Merchant Link, LLC
Moneris Solutions Corp
MoneyGram International
Nationwide Mutual Insurance Company
NBCUniversal
NCC Group Plc
Nets Oy
Nettitude Ltd
Nexusguard Consulting Limited
NIC Inc.
Nixu Ltd
North Carolina State University
NTT Data Intellilink Corporation
NTT Security Ltd
Paymetric Inc
PayPal Inc.
PayUSA
Pen Test Partners
PetSmart, Inc.
Philips Electronics North America Corporation
Phillips Consulting Ltd
Post Office
PowerPay, LLC
Praetorian Secure, LLC
PriceWaterhouseCoopers (PWC)
Privity Systems Inc.
Progressive Casualty Insurance Company
Promocion y Operations SA de CV
Protiviti
Rackspace
Rapid7 LLC
RBC Royal Bank
RBS
Retalix Inc.
RightScale Inc.
Rockwell Collins
RSM US, LLP
SecureConnect Inc.
SecureWorks, Inc.
Securisea, Inc.
SecurityMetrics, Inc.
Security Risk Management
Sense of Security Pty Ltd
ServerChoice
Sikich LLP
SISA
SITA

SIX Payment Services Ltd
Solutionary, Inc.
Specialized Security Services, Inc.
Sprint Nextel
SRC Security Research & Consulting GmbH
SSH Corporation
State Farm Mutual Automobile Insurance Company
StoreFinancial Services
Suncor Energy Inc.
Symantec Corporation
SynerComm, Inc
SystemExperts Corporation
Sysnet Global Solutions
Sysxnet Limited DBA Sysnet Global Solutions
TD Bank NA
Telstra
Terra Verde LLC
Tevora Business Solutions, Inc.
Time Warner Cable
TouchNet Information Systems, Inc.
Trustwave Holdings, Inc.
TUI Travel Plc.
TUV SUD Management Service GmbH
UL Transaction Security
University of North Carolina at Chapel Hill
University of Oklahoma
U.S. Bancorp
Vectra Corporation Ltd.
Vendor Safe Technologies
VeriFone Inc.
Verizon/Cybertrust
VigiTrust
Visa
Vodafone
Vodat International Ltd
Voltage Security
Wal-Mart Stores Inc.
The Walt Disney Company
Wayne Fueling Systems
Web.com
Westpac Banking Corporation
WEX Inc.
WorldPay
Wyndham Worldwide
Xerox
Xpient Solutions LLC

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.