PCI 支付卡产业第三方服务供应商 TPSP 的管理与实践

作者：atsec 唐冬生

关键词：支付卡产业、PCI DSS、持卡人数据、数据安全、第三方服务提供商、TPSP、Service Provider、尽职调查、第三方服务供应商管理

atsec information security

Tel +86-10-53056681
Fax +86-10- 53056678

www.atsec.com

目录

1 引言

在这个互联网技术日新月异的时代，云服务的普及让机构（实体）越来越倾向于借助第三方服务提供商来实现核心业务流程的外包，比如基础设施即服务（IaaS: Infrastructure as a Service）、平台即服务（PaaS：Platform as a Service）和软件即服务（SaaS: Software as a Service）。这些不同形态的服务供应商可能代表企业处理敏感的持卡人数据，也有可能为保护这些数据的环境提供技术支持，由此，实体不仅增加了责任的广度，也可能面临更多来自网络安全方面的挑战。在支付卡行业，众多实体通过第三方服务提供商（TPSP: Third-Party Service Provider）来达成 PCI DSS（Payment Card Industry Data Security Standard）标准的要求。atsec 作为支付卡产业（PCI：Payment Card Industry）安全标准委员会（SSC：Security Standards Council）授权的合格安全性评估机构（QSA：Qualified Security Assessor）在协助不同实体进行 PCI DSS 合规建设过程中，也就第三方服务供应商管理积累了诸多最佳实践。

本文主要探讨如何识别在 PCI DSS 审核范围内的第三方服务提供商（TPSP），并且分享从引入 TPSP 到日常管理 TPSP 的一系列最佳实践方法，以达到 PCI DSS 的合规要求，最终确保持卡人数据（CHD: Cardholder Data）得到有效保护。

2 TPSP 概述

2.1 TPSP 的定义

根据支付卡行业安全标准委员会（PCI SSC: Payment Card Industry Security Standards Council）的词汇表，TPSP 定义如下：

Third-Party Service Provider (TPSP): *Any third party acting as a service provider on behalf of an entity. See Multi-Tenant Service Provider and Service Provider.*

根据定义，第三方服务提供商（TPSP）是指代表实体（Entity）充当服务提供商（SP: Service Provider）的任何第三方，在 PCI DSS 合规评估时，这里的“实体”用于表示正在接受 PCI DSS 审查的公司、组织或企业。只有具备服务提供商（SP）的特征，并且为公司、组织或企业提供服务的第三方才符合 TPSP 的定义。因此，在判断给实体提供服务的第三方是否属于 PCI DSS 中定义的 TPSP 之前，我们需要对服务提供商（SP）的概念和范围有清晰的理解。PCI SSC 的词汇表对服务提供商（SP）定义如下：

Service Provider: *Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data (CHD) and/or sensitive authentication data (SAD) on behalf of another entity. This includes payment gateways, payment service providers (PSPs), and independent sales organizations (ISOs). This also includes companies that provide services that control or could impact the security of CHD and/or SAD. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities.*

结合该定义及 PCI SSC 文件《Third-Party Security Assurance》的理解，服务提供商（SP）是一个商业实体，并不是支付品牌的一部分，该实体直接参与或代表另一个实体处理、存储或传输持卡人数据。服务提供商（SP）还包括那些提供控制或可能影响持卡人数据安全的服务公司，即任何为实体提供处理、存储或传输持卡人数据服务的第三方，或者提供可能对这些数据安全产生影响的控制服务的第三方，都可被归为 PCI DSS 标准合规中的 TPSP。

2.2 TPSP 的示例

基于 TPSP 所提供的服务种类及其在持卡人数据（CHD）或持卡人数据环境（CDE: Cardholder Data Environment）中的角色和影响，以下这些机构可能会被视为 PCI DSS 合规范围内的 TPSP。

- **涉及存储、处理和/或传输持卡人数据的机构:** 呼叫中心，E-commerce 支付提供商，欺诈验证服务，信用报告服务，催收机构，第三方处理商，提供处理网关服务的实体，第三方债务催收等。
- **涉及保护持卡人数据（CHD）的机构:** 提供电子和物理媒体安全销毁的公司，电子和物理媒体的安全存储设施，提供令牌化或加密转换持卡人数据的公司，SaaS 公司（电子商务、票务、IDS/IPS、SOC 等），密钥管理提供商等。
- **参与保护持卡人数据环境 （CDE） 的机构:** 基础设施服务提供商，管理防火墙/路由器提供商，安全数据中心托管提供商，监控关键安全警报的服务，如入侵检测系统（IDS）、防病毒、变更检测、合规性监控、审计日志监控等。

- **可能接触到 CHD 或 CDE 的机构：**提供管理 IT 交付渠道和服务的提供商，提供软件开发的公司，如 Web 应用程序，提供维护服务的提供商，例如 HVAC 或清洁服务等。
- **提供销售点（Point-of-Sale）解决方案的机构：**通常涉及硬件和软件的安装、维护、监控，帮助商家处理交易、管理库存和跟踪销售数据集成商/经销商等。

通常情况下，TPSP 是一个在法律上独立运作的实体。然而，它也可能属于某个实体的内部部门或业务单元，尤其是当这个内部服务单元并不完全处于实体直接管理控制时，该部门或业务单元同样可以被视作 TPSP 的一种。还需要特别指出的是卡品牌及仅涉及提供公共网络接入的机构（如电信公司）不属于 TPSP。

2.3 TPSP、SP 和 Entity 三者之间的关系

了解 TPSP、SP 和 Entity 之间的相互影响和作用，对于深入理解 TPSP 的角色至关重要。

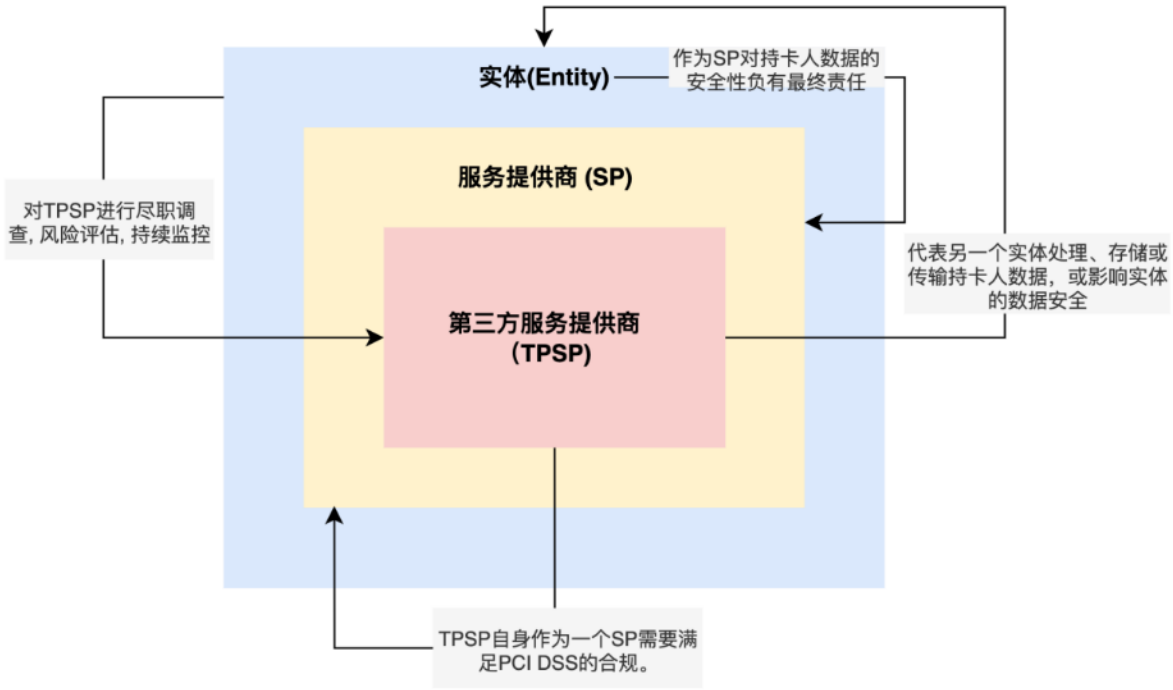

图 1：TPSP，SP 和 Entity 的关系图

基于上图，针对三者之间的关系说明如下：

a. 实体可能会与一个或多个服务提供商（SP）建立合作关系，以支持其业务运营。
b. TPSP 是服务提供商（SP）的一个子集。
c. 实体对确保其持卡人数据的安全性有最终责任，即使这些数据或 CDE 的管理是由 TPSP 执行的。
d. 实体必须确保其 TPSP 遵守 PCI DSS 的要求，并可能需要进行尽职调查、风险评估和持续监控，以确保 TPSP 的服务不会影响实体自身的 PCI DSS 合规性。
e. TPSP 也可能自身作为一个 SP 需要满足 PCI DSS 的合规。

3 有效识别 PCI DSS 范围内的 TPSP

在与第三方服务提供商（TPSP）合作之前，确保客户的帐户数据（Account Data）的安全是实体的重要任务。为此，实体必须制定一套完善的选择 TPSP 的政策和程序，并进行全面的尽职调查和风险评估，这不仅有助于判断该 TPSP 是否被纳入 PCI DSS 的审核范围，而且还能帮助实体进一步判断是否需要要求该 TPSP 遵守 PCI DSS 安全标准。在引入 TPSP 之前可以根据以下几个问题来判断 TPSP 是否在 PCI DSS 的审核范围内且需要满足标准的要求。如果某一个答案是肯定的，则该 TPSP 属于 PCI DSS 的审核范围：

a. TPSP 是否会存储、处理或传输 CHD？
b. TPSP 是否会参与对 CHD 的保护或访问？
c. TPSP 是否会参与对 CDE 的保护或访问？
d. TPSP 是否有访问 CDE 的可能性？

下述流程图，可以用来分析 TPSP 是否在 PCI DSS 审核范围内。

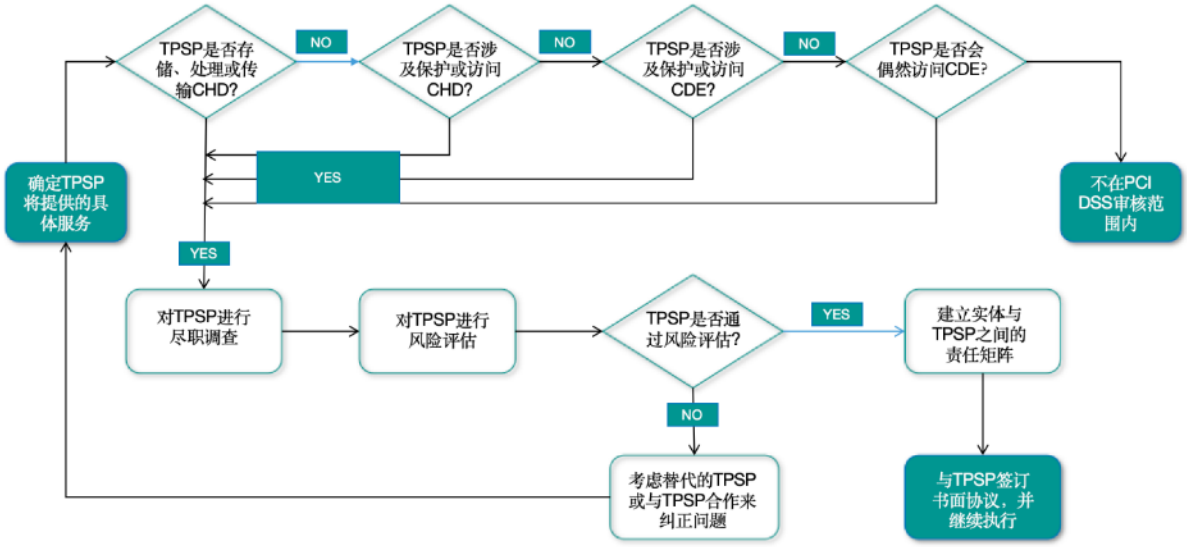

图 2：TPSP 是否在 PCI DSS 审核范围的分析流程图

4 PCI DSS 中对于实体采用的 TPSP 的管理要求及实践

当实体采用一个或多个第三方服务提供商（TPSP）来处理与其持卡人数据环境内或持卡人数据环境相关的功能时，这些 TPSP 的活动会直接影响实体的 PCI DSS 合规性，特别是与 PCI DSS 要求项 12.8 相关的对 TPSP 的风险管理。这意味着实体必须确保 TPSP 理解而且遵守 PCI DSS 的要求，以降低潜在的合规风险。

PCI DSS v4.0.1 标准 12.8 要求项包括 12.8.1-12.8.5，一共 5 个小项的要求，现逐项分析并分享最佳实践。

4.1 标准要求 12.8.1 及实践分享

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface. **Examples** Different types of TPSPs include those that:
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	**12.8.1.a** Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	

最佳实践：

为满足这一标准要求点，实体需要提供一份详细的第三方服务供应商清单，清晰地列出每个 TPSP 所提供的服务内容，重点关注每个 TPSP 的帐户数据的交互以及对 CDE 的安全影响。通常，实体可以通过采购清单系统或电子表格来记录这些信息，但需要确保信息的定期更新。而采用版本控制机制并始终保持最新状态可以有效地证明清单得到了妥善维护。

根据 PCI SSC 的参考文件《Information Supplement: Third-Party Security Assurance》6.1.2 章节的指导以及 atsec 多年合规审核经验的积累，对 TPSP 的以下基本信息进行收集及模板分享:

基本要素	中文说明	详情填写示例（填写时请替换示例内容）
TPSP Name	第三方服务提供商名称	[例如：XYZ 云服务提供商]
Primary Contacts	主要联系人信息	[例如：联系人姓名，职位，电子邮件，电话]
Services Provided	提供的服务	[例如：支付处理，数据存储，网络安全服务]
Shared Data Elements	共享的数据元素	[例如：敏感认证数据，主账号号码（PAN），有效期]
Data Location	数据存放位置	[例如：实体内部，第三方服务提供商位置，外部托管服务提供商]
System Components Reviewed	系统组件审核	[例如：服务器，数据库，网络设备]

TPSP Risk Assessment Results	TPSP 风险评估结果	[例如：低风险，中风险，高风险]
Monitoring Cycle Frequency	监控周期频率	[例如：每月，每季度]
Last Date of Review	最后审核日期	[具体日期，如：2024-10-01]
Contract Renewal/Expiry	合同续签/到期	[例如：2025-01-01 续签，2024-12-31 到期]
Required Documentation/Evidence	所需文件/证据	[例如：服务协议，安全政策，合规性证明]
Nested TPSPs	嵌套的 TPSPs	[例如：数据存储子服务提供商 A 公司，网络安全子服务提供商 B 公司]
Third-Party Payment Applications	第三方支付应用程序	[例如：XYZ 支付网关，ABC 移动支付应用]
Cardholder Data Volume	持卡人数据量	[例如：存储量 100GB，处理量 500 万笔交易]
Logical Network Access	逻辑网络访问	[例如：通过 VPN 访问，使用特定 IP 地址范围]
TPSP Designations Supporting PCI DSS Compliance	支持 PCI DSS 合规的 TPSP 认证	[例如：ISO, PCI QIR, PCI PTS, FIPS 140, 等等]

请注意，这个表格模板需要根据您实体的具体信息进行填写和调整。上述示例内容仅供格式参考，具体填写时请替换为实际数据。

4.2 标准要求 12.8.2 及实践分享

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	**12.8.2.a** Examine policies and procedures to verify that processes are defined to maintain written agreements with all TPSPs in accordance with all elements specified in this requirement. **12.8.2.b** Examine written agreements with TPSPs to verify they are maintained in accordance with all elements as specified in this requirement.	The written acknowledgment from a TPSP demonstrates its commitment to maintaining proper security of account data that it obtains from its customers and that the TPSP is fully aware of the assets that could be affected during the provisioning of the TPSP's service. The extent to which a specific TPSP is responsible for the security of account data will depend on the service provided and the responsibilities agreed between the provider and assessed entity (the customer). In conjunction with Requirement 12.9.1, this requirement is intended to promote a consistent level of understanding between parties about their

最佳实践：

为了有效实施 PCI DSS v4.0.1 要求项 12.8.2，接受评估的实体应建立全面且系统的方法来管理第三方服务提供商（TPSP），以下是实体在书面协议签订方面可以采取的关键步骤和策略：

a. **TPSP 的识别**：必须首先识别处理帐户数据或可能影响持卡人数据环境（CDE）安全的所有 TPSP。这涉及对所有第三方关系进行彻底评估，以了解他们在帐户数据和 CDE 方面的角色和责任。

b. **制定书面协议**：与每个 TPSP 制定详细的书面协议。这些协议应明确规定 TPSP 对保护其拥有、处

理、传输或可能影响实体 CDE 安全的帐户数据的责任。至关重要的是，这些协议必须根据每个 TPSP 提供的特定服务以及所涉及的数据安全风险进行定制。

c. **TPSP 的确认**：确保每个 TPSP 正式确认其对帐户数据安全的责任。该确认应成为书面协议的一部分。必须确保此确认清晰并与所提供的服务和分配的职责保持一致。

d. **协议的定期审查和更新**：制定政策和程序来定期审查和更新这些协议，以反映服务、数据处理实践或合规性要求的任何变化。

e. **监控和验证**：实施持续监控和验证 TPSP 遵守协议的流程。这可能涉及对 TPSP 遵守 PCI DSS 要求的情况进行定期评估、审计或审查。

f. **管理嵌套关系**：如果 TPSP 依赖其他第三方提供商（"nested" TPSPs）来提供服务，请确保这些嵌套关系也包含在协议中。主要 TPSP 应提供与其分包商签订类似书面协议的证据。（"nested" TPSPs） 是指为提供服务而与另一家第三方服务提供商签订服务合同的任何实体。）

g. **文档和证据存储**：为所有书面协议、确认书和相关文档维护一个存储库。该存储库应定期更新，并在 PCI DSS 评估期间轻松访问以供审查。

h. **培训和意识**：对参与管理 TPSP 关系的员工进行定期培训和意识教育，以确保他们了解这些协议的重要性以及他们在维护这些协议中的作用。

i. **利用指导资源**：利用《Information Supplement: Third-Party Security Assurance》等 PCI SSC 官方的资源，获取有关有效管理 TPSP 关系的更多方法和指导。

另外，为满足 PCI DSS 要求点 12.10 中对事件响应计划的标准要求，对于疑似的数据泄露事件，可能需要在此类外泄事件发生后的最短时间内采取具体行动。因此，强烈建议实体在与 TPSP 签订的合同中规定，在发生违规/泄露事件时，TPSP 必须全面参与 PCI 取证调查（PFI: PCI Forensic Investigator）的相关工作，包括协助提供实体的数据、系统、组件和相关服务的信息以供调查。

4.3 标准要求 12.8.3 及实践分享

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	**12.8.3.a** Examine policies and procedures to verify that processes are defined for engaging TPSPs, including proper due diligence prior to engagement	A thorough process for engaging TPSPs, including details for selection and vetting prior to engagement, helps ensure that a TPSP is thoroughly vetted internally by an entity prior to

最佳实践:

为了符合 PCI DSS 的 12.8.3 标准项要求，实体需要制定一个全面的 TPSP 管理计划，其中包括在利用任何第三方服务提供商的 PCI DSS 服务前，进行全面的评估和审查。这要求实体不仅要有一套明确的政策和程序来指导尽职调查的步骤，还要能够证明其实践是充分的，以确保 TPSP 达到既定的安全标准。此外，实体的政策还应详细说明评估标准、所需从 TPSP 收集的信息类型，以及如何验证 TPSP 保护帐户数据的能力、PCI DSS 合规状态和其它相关的安全措施。

以下在与 TPSP 合作之前的调查步骤可以供实体进行参考。

a. **确定服务范围**：确定 TPSP 在存储、处理或传输持卡人数据方面的参与程度以及对持卡人数据环境

（CDE）安全的影响。

b. **初步审查：**在建立合作之前，初步审查 TPSP 以确保与其合作不会对实体的 PCI DSS 合规性产生负面影响。可以针对性的进行财务稳定性、公司声誉、违规（如果有发生）以及每次违规的补救状态、退出策略（考虑在合作关系需要终止时的退出策略和流程）、业务连续性等风险因素的审查（这些风险因素可能超出了 PCI DSS 要求的范围）。

c. **咨询收单行或支付卡品牌：**了解 TPSP 服务是否被收单行或支付卡品牌批准使用，以及是否有关于使用该 TPSP 的限制。

d. **审查 TPSP 验证文件：**请求 TPSP 提供证明其符合 PCI DSS 的验证文件，如合规性证明（AOC：Attestation of Compliance），自我评估调查问卷（SAQ-D），ASV （Approved Scanning Vendor）扫描报告等，并检查 AOC 的 2a 章节“Scope Verification”中评估的服务名称和类型，以验证该 TPSP 提供的服务是否涵盖在内。

e. **查阅支付卡品牌维护的验证服务提供商列表和网站：**查看支付卡品牌是否维护了 TPSP 的验证列表，并了解这些列表的范围。

f. **风险评估：**基于行业接受的方法对 TPSP 进行全面的风险评估，以了解与之合作相关的风险水平。

g. **文档化结果：**记录尽职调查的结果，包括 PCI DSS 合规性验证的过期日期、验证供应商、获取银行、审计范围等。

以下流程图呈现了实体在对潜在的第三方服务提供商（TPSP）进行尽职调查时需要遵循的步骤。（流程仅供参考，每个实体都应该根据自己的持卡人数据环境确定适当的尽职调查流程。）

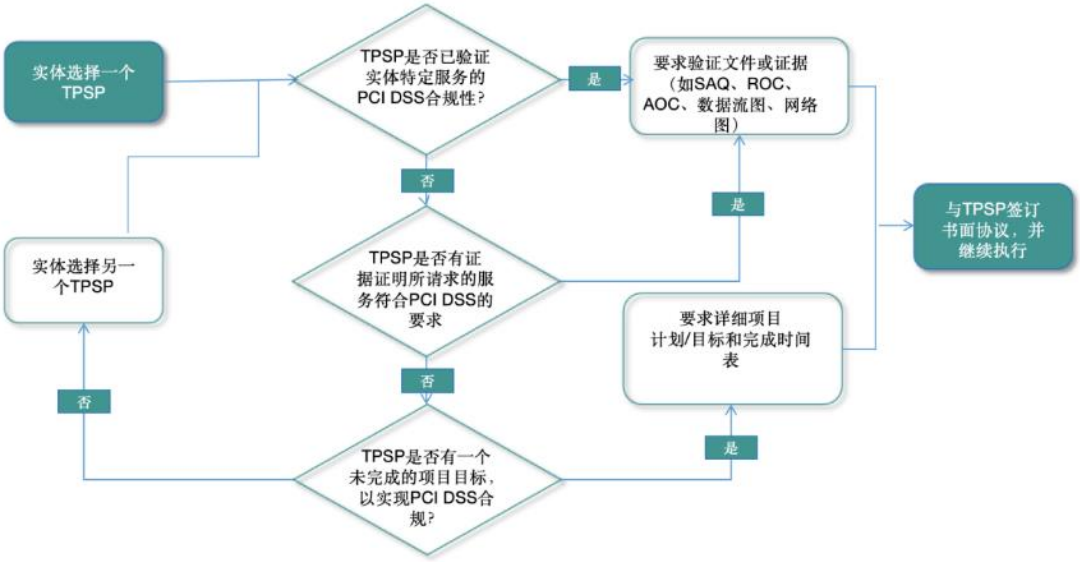

图 3：针对 TPSP 尽职调查过程示例

4.4 标准要求 12.8.4 及实践分享

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	**12.8.4.a** Examine policies and procedures to verify that processes are defined to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness about whether they comply with the requirements applicable to the services they offer to the organization.

最佳实践:

PCI DSS 标准要求 12.8.4 并未指定被审核实体的 TPSP 必须符合 PCI DSS 标准，仅指定被审核实体按照要求中指定的方式监控其合规性状态。因此，实体无需验证 TPSP 是否符合 PCI DSS 即可满足要求 12.8.4。但是，如果 TPSP 通过提供某一项服务来满足实体的 PCI DSS 要求，则这项由 TPSP 提供的服务在实体的 PCI DSS 评估的范围内，这项 TPSP 的服务的合规性也将影响实体的合规性。

例如，如果实体使用 TPSP 来管理其网络安全控制，而 TPSP 没有提供证据证明其满足 PCI DSS 要求 1 中的适用要求，则这些要求项对实体的评估来说是不满足 PCI DSS 标准要求的。

再举一个例子，代表实体存储持卡人数据备份的 TPSP 需要满足与访问控制、物理安全等相关的适用要求，以便其客户在 PCI DSS 合规评估时符合这些要求项。

另外需要特别提醒的是当 PCI DSS 标准的新版本发布，实体开始过渡到新版本的 PCI DSS 时，可能会出现实体依赖已合规旧版本 PCI DSS 标准的 TPSP 的情况。在这种情况下，TPSP 的 PCI DSS 验证必须在其所使用的标准版本停用之前完成，并且其验证必须仍然是最新的（即，自服务提供商验证以来尚未过去 12 个月）。

4.5 标准要求 12.8.5 及实践分享

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	**12.8.5.a** Examine policies and procedures to verify that processes are defined to maintain information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both the TPSP	It is important that the entity understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the entity, and for those that are shared, specifics about how the

最佳实践:

PCI DSS 责任矩阵有助于明确实体和第三方服务提供商（TPSP）在维护 PCI DSS 标准要求上的责任分配。包括但不限于以下责任应在正式的书面协议中详细列明：

a. TPSP 是否执行/管理/维护所需的控制？
b. 控制是如何实现的，支持过程是什么？补丁更新的过程是否包括测试、调度、批准等细节？
c. TPSP 将如何以及何时向实体提供持续的保证和/或证据，以满足控制要求？例如，定期报告、实时通知、测试结果等。

以下 PCI DSS 责任矩阵样本作为一个示例，供实体与 TPSP 沟通时参考，以便明确每个 PCI DSS 要求项的责任归属和相关注意事项。

标准要求项	责任方			实体责任的具体覆盖/范围	TPSP 责任的具体覆盖/范围	TPSP 将如何以及何时向实体提供合规证据
	TPSP	实体	共有			
1.1.1						
1.1.2						
1.2.1						
1.2.2						
1.2.3						
1.2.4						
1.2.5						
1.2.6						
1.2.7						
1.2.8						

注：这份责任矩阵示例供实体和/或第三方服务提供商（TPSP）根据自身判断选择性使用；完成此责任矩阵并不是强制性的，实体或 TPSP 不必通过完成此责任矩阵来满足任何 PCI DSS 要求。

5 PCI DSS 中对于 TPSP 的要求及实践分享

PCI DSS v4.0.1 要求项 12.9 指出，对于正在接受评估的实体，如果自身作为 TPSP，必须满足一系列标准以支持其客户的 PCI DSS 合规性。要求包括 12.9.1 和 12.9.2。现逐项分析并分享最佳实践。

5.1 标准要求 12.9.1 及最佳实践

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.9.1 ***Additional requirement for service providers only:*** TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.	**12.9.1** ***Additional testing procedure for service provider assessments only:*** Examine TPSP policies, procedures, and templates used for written agreements to verify processes are defined for the TPSP to provide written acknowledgments to customers in accordance with all elements specified in this requirement.	In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between TPSPs and their customers about their applicable PCI DSS responsibilities. The acknowledgment from the TPSP evidences the TPSP's commitment to maintaining proper security of the account data that it obtains from its customers. The TPSP's internal policies and procedures related to their customer engagement process

最佳实践：

为了有效实施 PCI DSS v4.0.1 的要求 12.9.1，第三方服务提供商（TPSP）应建立一个明确的流程，以正式确认其对客户的安全责任。以下是确保符合该要求的结构化方法：

a. **政策和程序制定：**制定全面的政策和程序，明确向客户提供书面确认的流程，包括起草、审核和发送确认的角色和责任。
b. **确认模板创建：**创建书面的模板，确保其灵活性以适应不同的服务协议和客户需求，涵盖服务提供商在保护帐户数据方面的关键责任。
c. **确认内容定制：**根据与客户的具体协议定制每份确认，反映所提供服务的细节、TPSP 的数据访问和处理范围，以及与客户的持卡人数据环境（CDE）相关的特定责任。
d. **法律和合规审查：**由法律和合规团队审核书面确认，确保其符合合同义务并遵循 PCI DSS 标准。
e. **与客户协议整合：**将确认内容纳入与客户的服务协议或合同中，使其成为 TPSP 与客户之间的正式协议的一部分。
f. **文档和记录保存：**保存所有发送给客户的书面确认记录，作为 TPSP 文档流程的一部分，便于审计。
g. **持续更新和审查：**定期审查和更新流程和模板，以确保持续符合 PCI DSS 标准及法律或监管要求的变化。
h. **审计和评估准备：**准备向合格安全评估师（QSA）展示这些流程和文档，确保证据和回答与要求的意图一致。
i. **与客户沟通：**与客户沟通，阐明这些确认事项（acknowledgments）的重要性，以及它们如何助力提升整个持卡人数据环境的安全性。

实施 PCI DSS 要求 12.9 不仅仅是为了达到合规标准，更是为了培训和提高团队的安全意识。TPSP 必须认识到，这些确认事项是保护持卡人数据和维护客户信任的一部分，是更广泛的客户承诺中的重要组成。

5.2 标准要求 12.9.2 及最佳实践

标准规定的方法要求:

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations. **Good Practice** If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, they may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the
12.9.2 ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data or sensitive authentication data.	12.9.2 ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.	

最佳实践:

当 TPSP 协助客户进行 PCI DSS 合规性评估时，他们有义务提供确凿的证据，证明其服务完全被纳入客户的 PCI DSS 评估范围内，并且相关的安全标准已经过彻底审查和验证。

如果 TPSP 拥有 PCI DSS 合规性证明（AOC），应根据客户需求提供，以证明其服务满足 PCI DSS 的相关要求。此外，如果客户为验证相关的服务在 PCI DSS 合规审核范围内，客户也可以索取 TPSP 的合规性报告（ROC: Report on Compliance）的相关部分内容，或服务提供商自我评估问卷（SAQ-D）的相关部分。

如果 TPSP 尚未进行 PCI DSS 评估或没有适用的 AOC 时，他们应向客户提供与 PCI DSS 要求相关的具体证据。这可能包括内部政策、程序、测试结果或第三方审计报告，以便客户（或其评估人员）能够确认 TPSP 符合这些 PCI DSS 要求。决定 TPSP 是否需要进行 PCI DSS 评估的权力在于管理合规性计划的组织，如收单行或支付卡品牌。因此，TPSP 应与这些组织直接沟通，了解具体要求，来确保其服务能够满足客户的合规性需求。

6 结语

为了确保支付卡数据的安全，持续合规 PCI DSS 标准对于处理帐户数据的 TPSP 至关重要。有效的 TPSP 管理不仅有助于实体符合 PCI DSS 要求，降低数据泄露和安全事件的风险，而且可以帮助实体有效的降低合规风险和法律责任。实体通过识别、评估和减轻风险，维护供应链安全，提高事件响应能力，进行持续监控和评估，以及保护实体的声誉，对于维护整个支付生态系统的安全也是至关重要的。

atsec 期待结合多年来 PCI DSS 合规方法论的积累，有效地帮助实体创建和管理 TPSP 流程和制度。

A 参考资料

(i) PCI SSC 的词汇表 https://www.pcisecuritystandards.org/glossary

(ii) Third-Party Security Assurance, v1.1, March 2016

(iii) Payment Card Industry Data Security Standard, v4.0.1, June 2024

(iv) PCI SSC 官网 FAQ 1065 How are third-party service providers (TPSPs) expected to demonstrate PCI DSS compliance for TPSP services that meet customers' PCI DSS requirements or may impact the security of a cardholder data environment?

(v) PCI SSC 官网 FAQ 1576 What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance?

(vi) PCI SSC 官网 FAQ 1312 How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)?

(vii) PCI SSC 官网 FAQ 1282 Can an entity be PCI DSS compliant if they use a third-party service provider (TPSP) that is validated to a previous version of PCI DSS?

(viii) PCI-DSS-Scoping-and-Segmentation-Guidance-for-Modern-Network-Architectures, September, 2024