

# Requirement 12 Continued: Third Party Service Providers (12.8 12.9)

---



**John Elliott**

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire [www.withoutfire.com](http://www.withoutfire.com)





## Requirement 12.8

Manage third party service providers



## Requirement 12.8

Maintain and implement policies and procedures to manage service providers

- with whom cardholder data is shared,
- or that could affect the security of cardholder data, as follows:

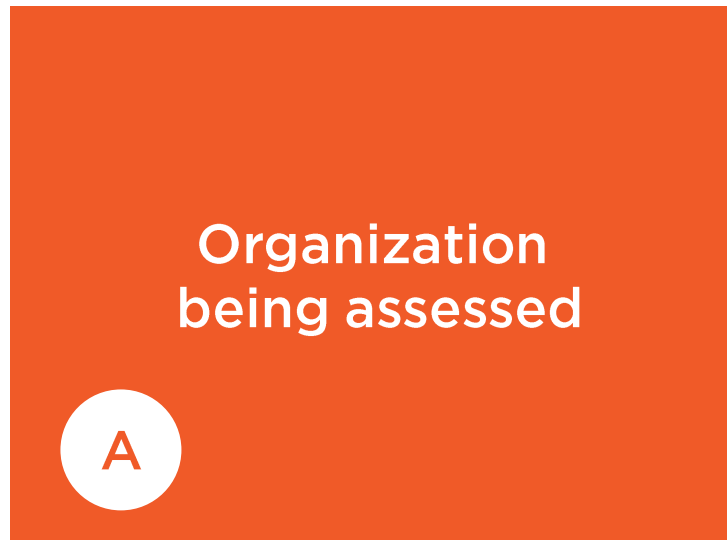


## Requirement Guidance

- If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers.
- Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc.

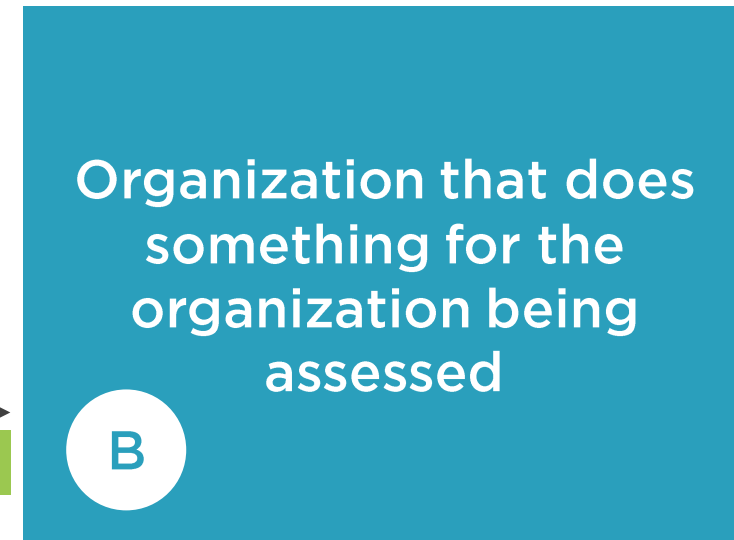
# What Determines a Service Provider?

“Customer” “Purchaser”

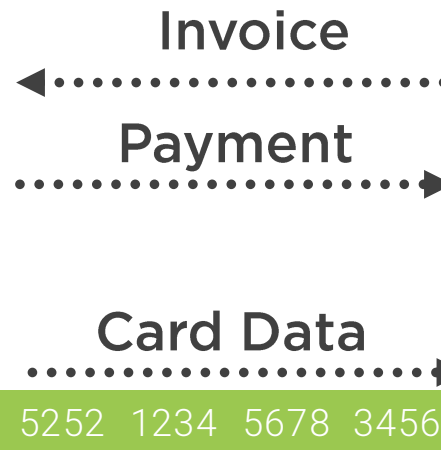


*Data Controller*

“Vendor” “Supplier”



*Data Processor*





[pcisecuritystandards.org/faqs](https://pcisecuritystandards.org/faqs)

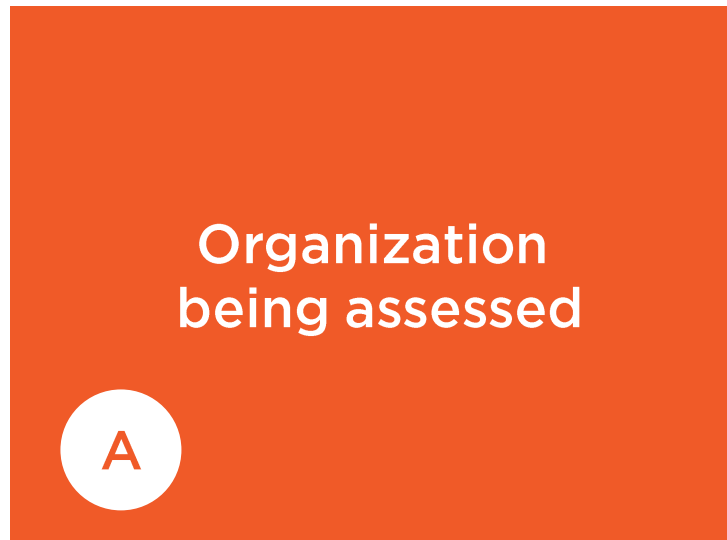
However, an entity that acquires a merchant's payment transactions and is defined by a payment brand to be an acquirer is not considered a service provider for that particular merchant's PCI DSS compliance for the purpose of Requirements 12.8

**FAQ 1284**



# A Common Error That QSAs Make

“Customer” “purchaser”

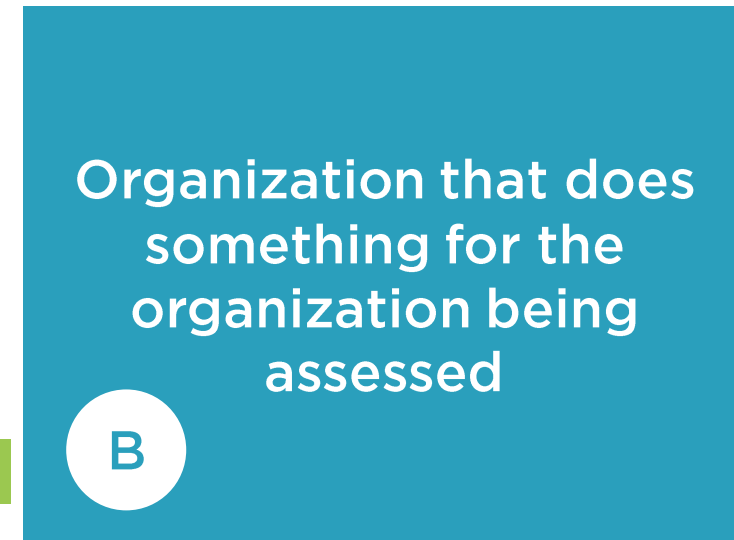


Invoice  
Payment

Card Data

5252 1234 5678 3456

“Vendor” “Supplier”



## 12.8 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Policies and procedures</b>
<b>Examine records</b>	<b>Y</b>	<b>Supporting documents</b>
<b>Interview people</b>	<b>-</b>	





### Requirement 12.8.1

Maintain a list of service providers including a description of the service provided.

**I also keep these in my list:**

**Contact information**

**What data and volume**

**When their compliance expires**



### Requirement Guidance

- Keeping track of all service providers identifies where potential risk extends to outside of the organization.



## 12.8.1 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	-	
<b>Examine records</b>	Y	Service provider list
<b>Interview people</b>	-	





## Requirement 12.8.2

~~Have a contract with the service provider that compels them to comply with PCI DSS~~

Have a written agreement with the service provider



## Requirement 12.8.2

Maintain a **written agreement** that includes an acknowledgement that the service providers are **responsible for the security of cardholder data** the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.



## Requirement Guidance

- The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity.
- In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities.



## 12.8.2 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	<b>Y</b>	<b>Written agreements</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	

Requirement 1 | Install and maintain a firewall configuration to to protect cardholder data





### Requirement 12.8.3

Ensure there is an **established process** for **engaging service providers** including proper **due diligence** prior to engagement.



### Requirement Guidance

- The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider.
- Specific due-diligence processes and goals will vary for each organization. Examples of considerations include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their compliance and what evidence they will provide, etc.



## 12.8.3 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Policies and procedures</b>
<b>Examine records</b>	<b>Y</b>	<b>Evidence of prior due diligence</b>
<b>Interview people</b>	<b>-</b>	





#### Requirement 12.8.4

Maintain a program to **monitor service providers'** PCI DSS **compliance** status at least **annually**.



#### Requirement Guidance

- Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and in scope for the client's PCI DSS assessment.
- The specific information an entity maintains will depend on the agreement with their providers, type of service, etc. The assessed entity should understand which PCI DSS requirements their providers have agreed to meet.

## 12.8.4 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>Y</b>	<b>Policy documentation</b>
<b>Examine records</b>	<b>Y</b>	<b>Compliance status records</b>
<b>Interview people</b>	<b>-</b>	





**Does a service provider have to comply with PCI DSS?**

**PCI DSS applies to service providers' activities**

**EITHER: The service providers can provide their own Attestation of Compliance**

- But make sure that it covers the people, processes and technology being provided!

**OR: The organization can include the service providers' people, processes and technology in its own assessment**





### Requirement 12.8.5

Maintain information about **which** PC DSS **requirements are managed** by each **service provider**, and which are managed by the **entity**.

**i.e. A Responsibility Matrix**



### Requirement Guidance

- Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and in scope for the client's PCI DSS assessment.
- The specific information an entity maintains will depend on the agreement with their providers, type of service, etc. The assessed entity should understand which PCI DSS requirements their providers have agreed to meet.

# Responsibility Matrix



136	<b>8.4 Document and communicate authentication policies and procedures to all users including:</b> <ul style="list-style-type: none"> <li>■ Guidance on selecting strong authentication credentials</li> <li>■ Guidance for how users should protect their authentication credentials</li> <li>■ Instructions not to reuse previously used passwords</li> <li>■ Instructions to change passwords if there is any suspicion the password could be compromised.</li> </ul>	YES	YES
137	<b>8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:</b> <ul style="list-style-type: none"> <li>■ Generic user IDs are disabled or removed.</li> <li>■ Shared user IDs do not exist for system administration and other critical functions.</li> <li>■ Shared and generic user IDs are not used to administer any system components.</li> </ul>	YES	YES
138	<b>8.5.1 Additional requirement for service providers only:</b> Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.  <i>Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted. Note: Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.</i>	NA	YES
139	<b>8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:</b> <ul style="list-style-type: none"> <li>■ Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.</li> <li>■ Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.</li> </ul>	YES	YES
140	<b>8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:</b> <ul style="list-style-type: none"> <li>■ All user access to, user queries of, and user actions on databases are through programmatic methods.</li> <li>■ Only database administrators have the ability to directly access or query databases.</li> <li>■ Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).</li> </ul>	YES	NA



## 12.8.5 Testing Procedures

<b>Observe/examine systems and settings</b>	<b>-</b>	
<b>Examine documentation</b>	<b>-</b>	
<b>Examine records</b>	<b>Y</b>	<b>Requirements records</b>
<b>Interview people</b>	<b>-</b>	



### ***Use of Third-Party Service Providers / Outsourcing***

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are their customer's responsibility to include in their own quarterly scans.

Service providers are responsible for demonstrating their PCI DSS compliance, and may be required to do so by the payment brands. Service providers should contact their acquirer and/or payment brand to determine the appropriate compliance validation.

There are two options for third-party service providers to validate compliance:

- 1) **Annual assessment:** Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or
- 2) **Multiple, on-demand assessments:** If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s)

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and/or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*





## Requirement 12.9

### For Service Providers Only

Allow your customers to comply with PCI DSS.



## Requirement 12.9

*Additional requirement for service providers only:*

Service providers **acknowledge in writing** to customers that they are **responsible for the security of cardholder data** the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.



## Requirement Guidance

- *Note: This requirement applies only when the entity being assessed is a service provider.*
- Along with Requirement 12.8.2, 12.9 is intended to promote consistent understanding between service providers and customers about their applicable PCI DSS responsibilities. Service providers' acknowledgement evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients.
- The service provider's internal policies and procedures related to customer engagement and templates used should include provision of PCI DSS acknowledgement to their customers



## 12.9 Testing Procedures

<b>Observe/examine systems and settings</b>	-	
<b>Examine documentation</b>	Y	<b>Policies and procedures Templates</b>
<b>Examine records</b>	-	
<b>Interview people</b>	-	





# Assessing 12.8

