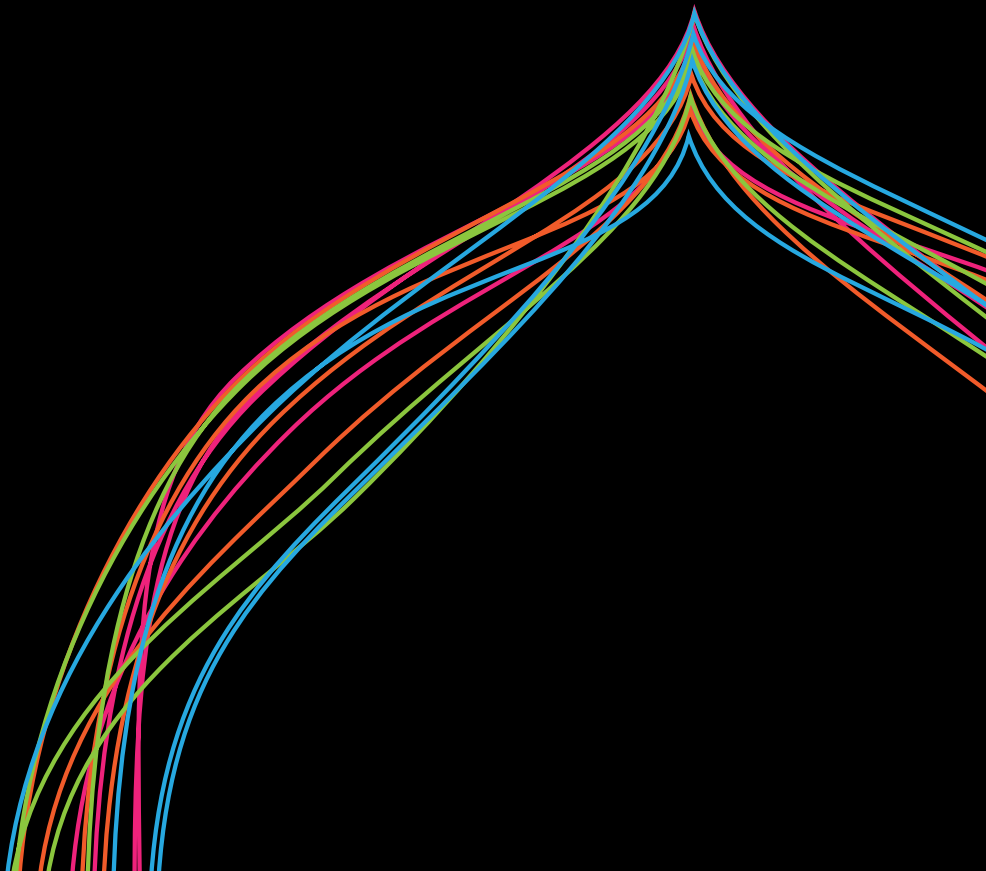


**Acquia®** THINK AHEAD.

# How to Achieve PCI DSS Compliance for Your Site in the Cloud

Brian Castagna, Senior Director of Information Security, Acquia



# Table of Contents

Introduction	3
PCI DSS Overview	3
PCI DSS in the Cloud Explained Step-by-Step	4
Benefits of Using a PCI DSS Compliant Cloud Service Provider	15
Conclusion	17
FAQ	17
Appendix A	19

# Introduction

*“International Retailer Hit by E-Commerce Credit Card Data Breach, CEO steps down.”* It’s the newspaper headline that no merchant ever wants to be a part of. Credit card data security breaches erode customer trust, carry costly fines and penalties, open legal liability and damage a merchant’s brand. The threat landscape is clear: criminal organizations employ highly skilled hackers to target merchants and steal credit card data. What is an organization’s best defense to these threats? The answer is: ensuring Payment Card Industry Data Security Standard (PCI DSS) security requirements are met to protect cardholder data along your entire payment lifecycle.

PCI DSS was created in 2004 to solve a challenge faced by the major card brands — American Express, Discover, JCB International, MasterCard and Visa Inc.: How do you unify a disparate set of individual card brand policies for cardholder data security to help ensure that merchants, card brands, and consumers alike are protected from fraud? The answer was PCI DSS. Major card brands came together and formed the [PCI Security Standards Council](#) to administer this global standard on their behalf. Over the years, the PCI Council has made incremental changes to the original standard to address the evolving threat landscape. However, the standard is still rooted in the original idea that merchants and service providers are operating predominantly on a traditional client/server technology stack interacting with only one or two service providers.

Fast Forward to 2016. The days of your cardholder data environment sitting in your corporate server farm managed by your system administrator are quickly coming to an end. Business leaders are asking themselves, *Why am I in the business of managing technology infrastructure, when my actual business is selling designer leather shoes?* Merchants and service providers are rapidly adopting cloud-computing services to leverage the efficiency, cost savings, flexibility, and enhanced cardholder data security found through technology service providers.

The use of numerous technology service providers presents a big challenge with PCI DSS in the cloud. How do organizations navigate the 250+ requirements for PCI DSS that **they are ultimately responsible for complying with** when they are outsourcing most of these responsibilities to third party providers?

This white paper is designed to provide organizations with insight and guidance into how they can successfully navigate the new challenges of PCI DSS in the cloud and achieve PCI DSS compliance.

## PCI DSS Overview

### WHAT IS PCI DSS?

It’s helpful to begin by reviewing the 12 requirements that comprise PCI DSS to ensure cardholder data security, and protect card brands, merchants, service providers, and consumers. The 12 requirements include coverage across the following six fundamental security areas:

#### PCI DATA SECURITY STANDARD — HIGH LEVEL OVERVIEW

##### Build and Maintain a Secure Network and Systems

Install and maintain a firewall configuration to protect cardholder data  
Do not use vendor-supplied defaults for system passwords and other security parameters

<b>Protect Cardholder Data</b>	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
<b>Maintain a Vulnerability Management Program</b>	Protect all systems against malware and regularly update anti-virus software or programs Develop and maintain secure systems and applications
<b>Implement Strong Access Control Measures</b>	Restrict access to cardholder data by business need to know Identify and authenticate access to system components Restrict physical access to cardholder data
<b>Regularly Monitor and Test Networks</b>	Track and monitor all access to network resources and cardholder data Regularly test security systems and process
<b>Maintain an Information Security Policy</b>	Maintain a policy that addresses information security for all personnel

The control coverage of the PCI DSS standard includes firewall and router configurations, encryption, vulnerability management, access, authentication, logging and monitoring, penetration testing, anti virus, security awareness training, policies, procedures, and other security requirements.

## TO WHOM DOES PCI DSS APPLY?

PCI DSS is very clear on the topic of to whom PCI DSS applies:

*“PCI DSS applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).”*

What does that mean for merchants that are using a cloud platform as a service provider like Acquia? It means that the merchant, the cloud platform as a service provider, the payment processor, and the infrastructure as a service provider need to **collectively** meet the PCI DSS requirements. We will explain this in more detail in the step-by-step example below.

## PCI-DSS in the Cloud Explained: Step-by-Step

### Step 1: Determine Your PCI DSS Merchant Level

Merchants fall into one of four levels based on their credit card transaction volume over a 12-month period. For the purpose of this cloud-focused whitepaper, we will only discuss e-commerce merchant transaction volume requirements.

To achieve or maintain PCI DSS compliance, merchants must meet specific validation requirements at each merchant level. According to the PCI council, validation requirements could include the completion of a self-assessment questionnaire (SAQ), a quarterly network scan by an Approved Scanning Vendor (ASV), and/or annual onsite audit performed by a third party qualified security assessor (QSA).

The table below explains the four merchant levels and validation requirements for each level:

Merchant Level	Card Brand	Merchant E-commerce Transaction Volume	Validation Requirements
1	Visa, MasterCard, Discover	Greater Than 6 Million Transactions	<ul style="list-style-type: none"> <li>• Annual Report on Compliance (ROC) to follow an on-site audit</li> <li>• Quarterly network scan by Approved Scan Vendor (ASV)</li> <li>• Attestation of Compliance (AOC) Form</li> </ul>
	American Express	Greater Than or Equal to 2.5 Million Transactions	
2	Visa, MasterCard, Discover	1–6 Million Transactions	<ul style="list-style-type: none"> <li>• Annual Self-Assessment Questionnaire (SAQ)</li> <li>• Quarterly network scan by ASV</li> <li>• AOC Form</li> </ul>
	American Express	50,000 to 2.5 Million Transactions	
3	Visa, MasterCard, Discover	20,000 to 1 Million E-commerce Transactions	<b>Visa, MasterCard, Discover, American Express:</b> <ul style="list-style-type: none"> <li>• Annual SAQ</li> <li>• Quarterly network scan by ASV</li> <li>• AOC Form</li> </ul>
	American Express	Less Than 50,000 Transactions	
4	Visa, MasterCard, Discover	Less than 20,000 E-commerce Transactions or All Other Merchants	<b>Visa Europe:</b> <ul style="list-style-type: none"> <li>• Use a service provider that has certified their PCI DSS compliance (<a href="http://www.visaeurope.com">www.visaeurope.com</a>)</li> <li>• Or, have certified their own PCI DSS compliance to the acquirer (who must, on request, be able to validate that compliance to Visa Europe)(SAQ)</li> </ul>

Did you find your e-commerce merchant level in the table above? If not, most organizations' accounting and finance departments should be able to provide you the transaction data over the prior 12 months.

## Step 2: Determine Your PCI Compliance Validation Types

Now that you have determined your e-commerce merchant level, the next step is to map that level to the correct validation type. There are two validation types:

### 1. A Self Assessment Questionnaire (SAQ):

- Designed for merchant levels 2, 3, and 4
- Intended to ease the validation burden for smaller merchants, but does not excuse the merchant's responsibility to ensure compliance with **ALL PCI DSS Requirements**.

### 2. An Onsite Audit:

- Designed for level 1 merchants and service providers or merchants that have suffered a breach of cardholder data

We've included the typical e-commerce validation types below.

Validation Type	Applicable Merchant Levels	Description
<b>SAQ A</b>	2, 3, 4	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels</i>
<b>SAQ A-EP</b>	2, 3, 4	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
<b>SAQ D Merchant</b>	2, 3, 4	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.
<b>Onsite Audit and ROC</b>	1	Onsite audit required to be performed by a third party QSA or qualified internal resource including the completion of the report on compliance (ROC) and attestation of compliance (AOC).

Let's discuss the differences between the e-commerce SAQ's above including SAQ A, SAQ A E-P and SAQ D.

We can start by bucketing SAQ A & A-EP into one grouping where the merchant is outsourcing some or all of cardholder data functions. In PCI DSS version 3 the PCI Council designed the new "SAQ A-EP" [highlighting the following deficiency in SAQ A](#):

*"Web servers did not have sufficient security controls applied to them and have become common targets for attackers as a means to compromise cardholder data security."*

In order to address the SAQ A deficiency, SAQ A-EP was designed for merchants that partially outsource cardholder data functions, including browser based posting methods such as Direct Post and Javascript to a PCI compliant payment processor. SAQ A was designed for merchants that completely outsource all cardholder data functions, including the use of an inline frame (iFrame) and/or URL redirect link to a PCI compliant payment processor. So what's the problem with this delineation between SAQ A and SAQ A-EP? Merchant web servers using an iFrame and/or URL redirect links are also susceptible to being attacked. In fact, it could be argued they are more susceptible than using Direct Post methods, because an attacker that owns the web server can redirect a user to a malicious payment page. So why do some merchants complete a shortened SAQ A when the same web server risks apply as merchants using browser based Direct Post or Javascript methods? It's a good question for the PCI Council, or your QSA, but Acquia's position is stated below:

Merchants should complete the more comprehensive SAQ A-EP to ensure the protection of their cardholder data. SAQ A-EP is explicitly designed for the partial outsourcing of cardholder data functions, and this is consistent with how Merchants use PaaS. The Merchant is ultimately responsible for ensuring all of the PCI DSS requirements are met, including validation that their third party web-hosting provider is PCI DSS compliant:

As stated as a requirement for SAQ-A EP:

*"If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements"*

SAQ D is a catch-all bucket typically reserved for merchants that are in fact storing, processing, and/or transmitting cardholder data on their merchant systems and/or have other non e-commerce methods of transacting cardholder data.

Regardless of the SAQ your organization completes, all Merchants are responsible to ensure that third party providers involved in cardholder data functions meet all applicable PCI requirements.

### Step 3: Implement the Required Controls and Complete the Relevant SAQ or ROC & AOC





Now that you have determined both your merchant level and PCI validation type, you must implement the required controls and complete the validation documentation: SAQ / ROC & AOC.

The SAQs and PCI DSS Requirements may be downloaded on the PCI Security Standards Council Website: [https://www.pcisecuritystandards.org/document\\_library](https://www.pcisecuritystandards.org/document_library)

Let's walk through an example of how to implement the PCI DSS requirements in the Cloud.

## THE PCI PLAYERS

To better understand the shared PCI responsibilities in the Cloud, let's set the stage by defining some of the common 'PCI Players':

	PCI Player	Example Player	Validation Type	Overview of PCI Responsibilities
	Merchant	Exotic Shoes Merchant Level 3	SAQ A-EP	Responsible for ensuring compliance with PCI DSS for their website. This includes both their organization's e-commerce applications and the end-to-end third party providers storing, processing, or transmitting cardholder data.  Responsible for application level security requirements.
	Platform as a Service (PaaS) Provider	Acquia Inc.	ROC	Responsible for the underlying platform: operating systems, LAMP stack, databases, firewalls, access and authentication, vulnerability management, security monitoring, etc.
	Infrastructure as a Service (IaaS) Provider	*Amazon Web Services (AWS)	ROC	Responsible for data center infrastructure including physical security, network, and routing, and certain encryption requirements.
	Payment Processor & Payment Gateway	Sally's Payments & Authorize.net	ROC	Typically responsible for all PCI DSS requirements. The payment processor and payment gateway are responsible for interfacing with the acquiring bank.

\*Acquia is ultimately responsible for the services that AWS provides. AWS is a sub-service provider of Acquia that is transparent to Acquia's customers. However, for

the purposes of PCI DSS it is important to delineate this separation of responsibility, as customers will need to rely on both the Acquia PCI Compliance & AWS PCI Compliance to achieve PCI compliance themselves.

Using our example “PCI Players’ above, let’s look how each of the 12 requirements would apply to them:

## 1. Install and maintain a firewall configuration to protect cardholder data

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)		
<b>PaaS</b> (Acquia)	✓	Acquia provides multiple layers of firewalls including AWS security group firewalls and IP table firewalls.
<b>IaaS</b> (AWS)	✓	The design of the AWS Cloud provides network layer protection against common network layer attacks. This includes layer two protections through the use of virtual switching.
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must maintain a firewall configuration to protect cardholder data.

## 2. Do not use vendor-supplied defaults for system passwords and other security parameters

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must not use any application level vendor-supplied defaults for system passwords and other security parameters.
<b>PaaS</b> (Acquia)	✓	Acquia does not use default system passwords in any Acquia host or software component.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must not use vendor-supplied defaults for system passwords and other security parameters.



### 3. Protect stored cardholder data

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes is responsible for cardholder data storage, retention, and certain key management requirements.  Acquia and AWS perform certain key management activities.
<b>PaaS</b> (Acquia)	✓	
<b>IaaS</b> (AWS)	✓	
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must protect stored cardholder data.

### 4. Encrypt transmission of cardholder data across open, public networks

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes, Acquia, and AWS perform certain encryption requirements.
<b>PaaS</b> (Acquia)	✓	
<b>IaaS</b> (AWS)	✓	
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must encrypt transmission of cardholder data across open, public networks.

## 5. Use and regularly update anti-virus software or programs

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must implement on-demand file scanning via a Drupal module.
<b>PaaS</b> (Acquia)	✓	Acquia runs vulnerability scans to detect malicious software.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must use and regularly update anti-virus software or programs.

## 6. Develop and maintain secure systems and applications

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes is responsible for application level system development requirements.
<b>PaaS</b> (Acquia)	✓	Acquia is responsible for platform level vulnerability monitoring, management, and response.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must develop and maintain secure systems and applications.

## 7. Restrict access to cardholder data by business need-to-know

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes is responsible for application level access control requirements to ensure that cardholder data is restricted by business need-to-know.
<b>PaaS</b> (Acquia)	✓	Acquia is responsible for access control requirements including security administration, restricted access, and role-based security.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net restrict access to cardholder data by business need-to-know.

## 8. Assign a unique ID to each person with computer access

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must meet application level authentication requirements and perform user access reviews.
<b>PaaS</b> (Acquia)	✓	Acquia must meet platform level authentication requirements and perform user access reviews.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must assign a unique ID to each person with computer access.

## 9. Restrict physical access to cardholder data

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)		
<b>PaaS</b> (Acquia)		
<b>IaaS</b> (AWS)	✓	AWS must restrict physical access to cardholder data.
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must restrict physical access to cardholder data.

## 10. Track and monitor all access to network resources and cardholder data

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must track and monitor all cardholder data at the application level.
<b>PaaS</b> (Acquia)	✓	Acquia must track and monitor all access to network resources and cardholder data at the platform level.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must track and monitor all access to network resources and cardholder data.

## 11. Regularly test security systems and processes

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must have vulnerability scans performed by an ASV and application layer penetration testing.
<b>PaaS</b> (Acquia)	✓	Acquia must meet vulnerability scanning, file integrity monitoring, and IDS requirements and have penetration testing performed.
<b>IaaS</b> (AWS)	✓	AWS must meet wireless security requirements.
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must regularly test security systems and processes.

## 12. Maintain a policy that addresses information security for employees and contractors

PCI Player	Responsibility	Summary
<b>Customer</b> (Exotic Shoes)	✓	Exotic Shoes must maintain policy that addresses information security for employees and contractors relevant to their application.
<b>PaaS</b> (Acquia)	✓	Acquia must maintain policy that addresses information security for employees and contractors relevant to their platform.
<b>IaaS</b> (AWS)		
<b>Payment Processor</b> (Sally's Payments) & <b>Payment Gateway</b> (Authorize.net)	✓	Sally's Payments and Authorize.net must maintain a policy that addresses information security for employees and contractors.

This overview of the 12 requirements should provide some additional context of why there are shared PCI DSS responsibilities in the Cloud. The example above describes high-level requirements for the merchant and different service providers in the chain. It makes sense that PCI requires each of these layers to be protected, as the weakest link in the chain could be exploited by an attacker and cardholder data could be breached at any layer.

(A more detailed responsibility matrix is included in Appendix A)

These 12 requirements are expanded upon and detailed in the PCI DSS standard documentation. The latest version of PCI DSS is 3.2, and you can download PCI DSS v3.2 from the PCI Security Council web site: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf)

#### Step 4: Conduct Quarterly Vulnerability Scans with a PCI DSS Approved Scanning Vendor

One specific requirement of PCI DSS worth highlighting is the use of an Approved Scanning Vendor (ASV).

ASV vulnerability scans must be performed on a quarterly basis for all merchant levels (1, 2, 3, 4) and e-commerce PCI DSS compliance validation types (SAQ A, SAQ A-EP, D Merchant, Onsite Audit and ROC).

##### What is the scope of the ASV Scans?

In our example, ASV scanning would need to be performed both for the customer (Exotic Shoes) web application and any web application management portals at the PaaS level (Acquia) that could have access into the cardholder data environment. The ASV scanning for the PaaS would be validated in their ROC during the annual onsite audit. The ASV scanning for the customer (Exotic Shoes) would need to be scheduled by the customer with an ASV scanning provider independent of their PaaS. Exotic Shoes would then work with both their internal development team to remediate any PCI ASV Scan findings, and/or their PaaS (Acquia) if it's a platform level configuration that needs to be addressed.

##### Why are ASV scans important?

Application level vulnerabilities are a common attack vector for threat actors interested in stealing your customers' cardholder data. The ASV scan identifies vulnerabilities to be reviewed and remediated or marked as a 'False Positive' by your scanning vendor.

##### Where can I find an Approved Scanning Vendor?

The list of Approved Scanning Vendors is available on the PCI Security Standards site at:

[https://www.pcisecuritystandards.org/assessors\\_and\\_solutions/approved\\_scanning\\_vendors](https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors)

#### Step 5: Review Service Provider, Payment Processor, and Payment Gateway PCI DSS AOCs

Ok — Great! You implemented the required controls for your PCI compliance type, completed your SAQ or ROC, and your ASV scanning is running. You're all set, right? Wrong.

Exotic Shoes is required to validate PCI DSS compliance for each of their service providers. PCI DSS is very clear on this topic in requirement 12.8 of [PCI DSS v3.2](#):

##### Requirement 12.8:

12.8 "Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data?"

##### What does requirement 12.8 mean?

Exotic Shoes must evaluate both service providers that are directly involved in storing, processing, or transmitting cardholder data such as the payment processor or certain hosting provider implementations (Sally's payments) OR service providers that could affect the security of the cardholder data such as your hosting provider that manages your web server or your infrastructure as a service provider (Acquia and AWS).

##### Requirement 12.8.4:

12.8.4 "Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?"

##### What does requirement 12.8.4 mean?

Exotic Shoes must validate PCI DSS compliance of service providers on an annual basis. In our example, this means that they should obtain an AOC or ROC from Sally's Payments, Authorize.net, Acquia and AWS to validate that all of their PCI DSS service providers are PCI DSS compliant.

**Requirement 12.8.5:**

12.8.5 “Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?”

**What does requirement 12.8.5 mean?**

Exotic Shoes must have documented which of their providers are responsible for which PCI DSS requirements. For Acquia customers — we have documented this in a matrix in Appendix A of this white paper for our customers to meet this requirement.

**PCI Supplemental Guidance on Shared Management E-Commerce Implementations:**

“3.4.3: Shared Management E-Commerce Implementations: Merchants should understand that outsourcing to a third party via a shared management implementation does not allow the merchant to outsource PCI DSS responsibility, regardless of whether a merchant is eligible to complete a self-assessment questionnaire (SAQ). With each of these shared-management implementations, there is still security risk for the merchant since weaknesses on the merchant’s website can lead to compromise of the payment card data during the transaction process.”

## Benefits Using a PCI DSS Compliant Cloud Service Provider

### TIME AND COST IMPLICATIONS OF ACHIEVING PCI COMPLIANCE

Achieving PCI compliance is a costly and time-consuming exercise. Most organizations either employ an in-house PCI specialist or use outside consultants that understand the complex standard and can lead an organization through the implementation of the applicable requirements. In many cases, there are architectural and engineering efforts required to segment the cardholder data network from an organization’s corporate network. Such efforts may require purchasing new hardware (servers, firewalls, routers, etc.), and software (monitoring systems - intrusion detection/prevention, file integrity, security information event management, vulnerability scanning tools, etc.).

Finally, organizations need to undergo annual penetration testing and have an ASV perform vulnerability scans of their production systems on a quarterly basis if they choose to host their own PCI environment. Results from the penetration testing and ASV scans need to be remediated before an organization can achieve or maintain compliance.

Once a PCI environment has been implemented, it needs to be validated with the completion of a SAQ or audited by an authorized PCI QSA in order to achieve compliance, and completed/audited annually thereafter to maintain compliance. Organizations will need to budget for annual PCI audits, and disruptions to their day to day operations while audits are taking place by the third party QSA. In addition, to help ensure that organizations do not fall out of compliance, there needs to be a continual focus on maintaining controls throughout the year.

By selecting a PCI DSS compliant set of service providers, organizations are able to leverage the technology and resources of their service providers to meet their requirements for PCI compliance. In the examples above, the merchant Exotic Shoes is mainly responsible for application level requirements, where network, system level, and physical security requirements are outsourced to PCI DSS compliant service providers.

### Example Annual Costs:

Description of Cost	Annual Cost for DIY or Self-Service	Annual Cost with a PCI DSS compliant PaaS/IaaS
PCI DSS Expert Consultant or Employee	\$120,000	\$30,000 (application only)
PCI Audit Fees	\$35,000	\$0
Engineering Employee Time To Maintain PCI Applications / Systems	\$110,000	\$25,000 (application only)
Security Tools (Firewalls, Intrusion Detection System, File Integrity Monitoring, Vulnerability Scanning, SIEM)	\$200,000	\$0
ASV Scanning Vendor	\$4,000	\$2,000 (application only)
Opportunity Cost	\$50,000	\$0
<b>Total Annual Cost</b>	<b>\$519,000</b>	<b>\$57,000</b>

## Cost of a Credit Card Data Breach

As a Merchant — you are ultimately responsible to the card brands if there is a credit card data breach. The implications of a credit card breach are serious and far-reaching, include fines for non-compliance, affected customer notifications, card reissuance, and credit monitoring for all affected parties.

There are also concerns about loss of consumer trust and reputational damage. According to the [2015 Verizon PCI Compliance Report](#), 69 percent of consumers would be less inclined to do business with a breached organization. [According to PwC](#), in 2015 there were 38 percent more security incidents detected than in 2014.

Don't let your organization be a part of that statistic. Use cloud service providers that have a team of specialists responsible for credit card data security to reduce the likelihood of having a credit card data breach. If your partners and customers lose trust in you, there's a greater likelihood they will take their business elsewhere.



## Conclusion

PCI compliance is critical for any organization that processes credit card information, not only for regulatory reasons, but because it offers peace of mind for your organization, your customers, your partners, and the market at large. It ensures that consumer credit card data is safe and secure in your hands, and eliminates an element of risk or concern about conducting business in this digital age. So why not run your business on a platform that offers a PCI compliant platform out of the box? Save your organization the work, the headaches, and the maintenance by letting a PCI DSS compliant cloud service provider manage it for you.

## Frequently Asked Questions

**Question:** How does Acquia implement a PCI DSS compliant platform environment?

**Answer:** For most organizations, the type of time and cost commitment to build a PCI compliant environment isn't realistic. It makes more sense to work with a platform provider that offers a PCI compliant environment for them to run their business on. Acquia's PCI compliant enterprise platform is that offering within a virtual private cloud (VPC). This offering provides significant time and cost savings, allowing your internal security team to focus on other more pertinent matters, and for the rest of your organization to run their business knowing that their data is secure.

**Question:** To Network Segment or Not Network Segment? That is the question.

**Answer:** Actually — it's more of a rhetorical question. Merchants and service providers ALWAYS want to employ network segmentation when possible to reduce the risk and scope of the cardholder data environment.

What is network segmentation? Network segmentation is a PCI term used to describe the reduction of the scope of your cardholder data environment to a logically segmented zone. For example, where would you keep your grandmother's diamonds in the house? Would you keep them scattered in jewelry boxes and desk drawers around the house? Or would you keep them in the half-ton safe in the basement? It's the same concept with cardholder data.

At Acquia we employ network segmentation using a virtual private cloud (VPC) that helps to ensure protection of our customers' cardholder data in an environment that can easily and quickly apply to the ever-evolving requirements of PCI DSS.

**Question:** A technology service provider is saying that they are PCI compliant because one of their sub-service providers is PCI compliant. Is that true — is the technology service provider compliant through association?

**Answer:** No. A common tactic for technology service providers that are not PCI DSS compliant is to refer to a sub-service provider's compliance and claim that compliance as their own. The most frequent example is organizations that state a data center provider's PCI audit or Service Organization Controls (SOC) audit provides the required coverage for their services. In most cases, the data center audit only includes controls around physical security (PCI Req #9), environmental security, and some networking controls (PCI Req #1). The scope of these data center audits typically does not include the application, operating system, or database layer PCI DSS security requirements. In general, your PaaS provider is responsible for the operating system and database security, and the customer is responsible for application level security.

**Question:** The design of my web application doesn't store, process, or transmit any cardholder data. Do I still need to have a PCI DSS compliant PaaS or IaaS with this design?

**Answer:** Yes. As mentioned in the details of the White Paper and related PCI DSS Security Council references:

- Per PCI DSS v3.2: "PCI DSS applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers."
- All Merchants are responsible for ensuring that third party providers involved in cardholder data functions meet all applicable PCI requirements.
- Most e-commerce customers using a PaaS/IaaS should be completing SAQ A-EP which states: "If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements"
- Requirement 12.8 of PCI DSS: "Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data" (e.g the webserver)

**Question:** My cloud provider is stating that I need separate dedicated hardware for PCI DSS compliance. Is that true?

**Answer:** Yes. PCI DSS requirement 2.2.1 requires 'process isolation.' This means that a PCI DSS compliant hosting stack is required to have separate and dedicated server infrastructure including web server, database server, and file server. PCI DSS requires this separation to help that ensure if one server is compromised, an attacker cannot easily move laterally to other parts of the cardholder data environment.

**Question:** A technology service provider is saying that PCI DSS does not apply to modern cloud architectures. Is that true?

**Answer:** No. PCI DSS must be applied to merchants, processors, acquirers, issuers, and service providers regardless of the design of their systems architecture.

**Question:** How does PCI DSS compare to and complement other security compliance standards?

**Answer:** The short answer is that PCI DSS is the least flexible of the common security compliance standards such as SSAE 16, SOC 2, ISO 27001, and FedRAMP. PCI DSS requirements are mandatory and must be in place for any and all organizations that store, process, or transmit cardholder data. Having a mandatory set of predetermined requirements is a sharp contrast from standards such as SSAE 16 or SOC 2 that allow a service provider to document their own security controls to meet control objectives or common criteria respectively. The rigidity of PCI is a double-edged sword; having a consistent baseline of security requirements helps to ensure the same set of security requirements are applied uniformly across merchants and service providers. However, this consistent baseline of security requirements was written in a pre-cloud world. The same pre-cloud world where your system administrator kept the cardholder data environment (CDE) padlock protected in a plexiglass box in the computer closet. Without flexibility, there is a risk that relevant organizational specific security controls are missed and not attested to by the merchant or service provider auditors.

**Question:** How do merchants protect against the risk that PCI DSS requirements do not capture the relevant controls of PCI DSS technology service providers?

**Answer:** Ask your service providers for their other security attestations such as SSAE 16, SOC 2, ISO 27001 to gain visibility into additional security controls that are not covered by PCI DSS.

## Appendix A

PCI in the cloud requires shared responsibilities. The responsibility matrix below outlines the PCI responsibility of Acquia, the Customer, and the Third Party IaaS provider:

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
<b>REQUIREMENT 1</b>			
1.1.1	X		X
1.1.2	X		
1.1.3	X		
1.1.4	X		
1.1.5	X		X
1.1.6	X		X
1.1.7	X		X
1.2.1	X		X
1.2.2			X
1.2.3			X
1.3.1	X		X
1.3.2	X		X
1.3.3	X		X
1.3.4	X		X
1.3.5	X		X
1.3.6	X		X
1.3.7	X		X
1.3.8	X		X
1.4.1	X		
1.5.1	X		

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
----------------	-----------------------	-------------------------	---------------------------------

## REQUIREMENT 2

2.1	X	X	
2.1.1			
2.2	X	X	
2.2.1	X		
2.2.2	X		
2.2.3	N/A	N/A	N/A
2.2.4	X	X	
2.2.5	X	X	
2.3	X		
2.4	X		
2.5	X	X	
2.6	N/A	N/A	N/A

## REQUIREMENT 3

3.1		X	
3.2		X	
3.2.1	X	X	
3.2.2	X	X	
3.2.3	X	X	
3.3		X	
3.4		X	
3.4.1	X	X	
3.5		X	X

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
3.5.1		X	X
3.5.2		X	X
3.5.3		X	X
3.6		X	X
3.6.1		X	X
3.6.2		X	X
3.6.3		X	X
3.6.4		X	X
3.6.5		X	X
3.6.6		X	X
3.6.7		X	X
3.6.8		X	X
3.7		X	X

#### REQUIREMENT 4

4.1	X	X	
4.1.1			X
4.2	N/A	N/A	N/A
4.3	X	X	

#### REQUIREMENT 5

5.1	N/A	N/A	N/A
5.1.1	N/A	N/A	N/A
5.1.2	X	X	
5.2	N/A	N/A	N/A

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
5.3	N/A	N/A	N/A
5.4	N/A	N/A	N/A

## REQUIREMENT 6

6.1	X		
6.2	X		
6.3		X	
6.3.1		X	
6.3.2		X	
6.4		X	
6.4.1		X	
6.4.2		X	
6.4.3		X	
6.4.4		X	
6.4.5	X	X	
6.4.5.1	X	X	
6.4.5.2	X	X	
6.4.5.3	X	X	
6.5.4.4	X	X	
6.5		X	
6.5.1		X	
6.5.2		X	
6.5.3		X	
6.5.4		X	
6.5.5		X	

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
6.5.6		X	
6.5.7		X	
6.5.8		X	
6.5.9		X	
6.5.10		X	
6.6		X	
6.7		X	

#### REQUIREMENT 7

7.1	X	X	
7.1.1	X	X	
7.1.2	X	X	
7.1.3	X	X	
7.1.4	X	X	
7.2.1	X	X	
7.2.2	X	X	
7.2.3	X	X	
7.3	X	X	

#### REQUIREMENT 8

8.1	X	X	
8.1.1	X	X	
8.1.2	X	X	
8.1.3	X	X	
8.1.4	X	X	

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
8.1.5	X	X	
8.1.6	X	X	
8.1.7	X	X	
8.1.8	X	X	
8.2	X	X	
8.2.1	X	X	
8.2.2	X	X	
8.2.3	X	X	
8.2.4	X	X	
8.2.5	X	X	
8.2.6	X	X	
8.3	X		
8.4	X	X	
8.5	X	X	
8.5.1		X	
8.6	X	X	
8.7	X	X	
8.8	X	X	

## REQUIREMENT 9

9.1			X
9.1.1			X
9.1.2			X
9.1.3			X



PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
9.2			X
9.3			X
9.4.1			X
9.4.2			X
9.4.3			X
9.4.4			X
9.5			X
9.5.1			X
9.6			X
9.6.1			X
9.6.2			X
9.6.3			X
9.7			X
9.7.1			X
9.8			X
9.8.1			X
9.8.2			X
9.9			X
9.9.1			X
9.9.2			X
9.9.3			X
9.10			X

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
<b>REQUIREMENT 10</b>			
<b>10.1</b>	X	X	
<b>10.2</b>	X	X	
<b>10.2.1</b>	X	X	
<b>10.2.2</b>	X	X	
<b>10.2.3</b>	X	X	
<b>10.2.4</b>	X	X	
<b>10.2.5</b>	X	X	
<b>10.2.6</b>	X	X	
<b>10.2.7</b>	X	X	
<b>10.3</b>	X	X	
<b>10.3.1</b>	X	X	
<b>10.3.2</b>	X	X	
<b>10.3.3</b>	X	X	
<b>10.3.4</b>	X	X	
<b>10.3.5</b>	X	X	
<b>10.3.6</b>	X	X	
<b>10.4</b>	X		
<b>10.4.1</b>	X		
<b>10.4.2</b>	X		
<b>10.4.3</b>	X		
<b>10.5</b>	X	X	
<b>10.5.1</b>	X	X	
<b>10.5.2</b>	X	X	

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
10.5.3	X	X	
10.5.4	X	X	
10.5.5	X	X	
10.6.1	X	X	
10.6.2	X	X	
10.6.3	X	X	
10.7	X	X	
10.8	X	X	

#### REQUIREMENT 11

11.1			X
11.1.1			X
11.1.2			X
11.2.1	X		
11.2.2	X	X	
11.2.3	X	X	
11.3	X	X	
11.3.1	X	X	
11.3.2	X		
11.3.3	X	X	
11.3.4	X		
11.4	X		
11.5	X		
11.5.1	X		
11.6	X	X	

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
<b>REQUIREMENT 12</b>			
<b>12.1</b>	X	X	
<b>12.1.1</b>	X	X	
<b>12.2</b>	X	X	
<b>12.3</b>	X	X	
<b>12.3.1</b>	X	X	
<b>12.3.2</b>	X	X	
<b>12.3.3</b>	X	X	
<b>12.3.4</b>	X	X	
<b>12.3.5</b>	X	X	
<b>12.3.6</b>	X		
<b>12.3.7</b>	X	X	
<b>12.3.8</b>	X	X	
<b>12.3.9</b>		X	
<b>12.3.10</b>	X	X	
<b>12.4</b>	X	X	
<b>12.5</b>	X	X	
<b>12.5.1</b>	X	X	
<b>12.5.2</b>	X	X	
<b>12.5.3</b>	X	X	
<b>12.5.4</b>	X	X	
<b>12.5.5</b>	X	X	
<b>12.6</b>	X	X	
<b>12.6.1</b>	X	X	

PCI Control ID	Acquia Responsibility	Customer Responsibility	Third Party IaaS Responsibility
12.6.2	X	X	
12.7	X	X	
12.8	X	X	
12.8.1	X	X	
12.8.2	X	X	
12.8.3	X	X	
12.8.4	X	X	
12.8.5	X	X	
12.9	X		
12.10	X	X	
12.10.1	X	X	
12.10.2	X	X	
12.10.3	X	X	
12.10.4	X	X	
12.10.5	X	X	
12.10.6	X	X	