The DIY Guide to PCI

IMPLEMENTING PCI COMPLIANCE IN THE CLOUD

A word of advice

Looking to go at it alone when securing your public cloud environment?

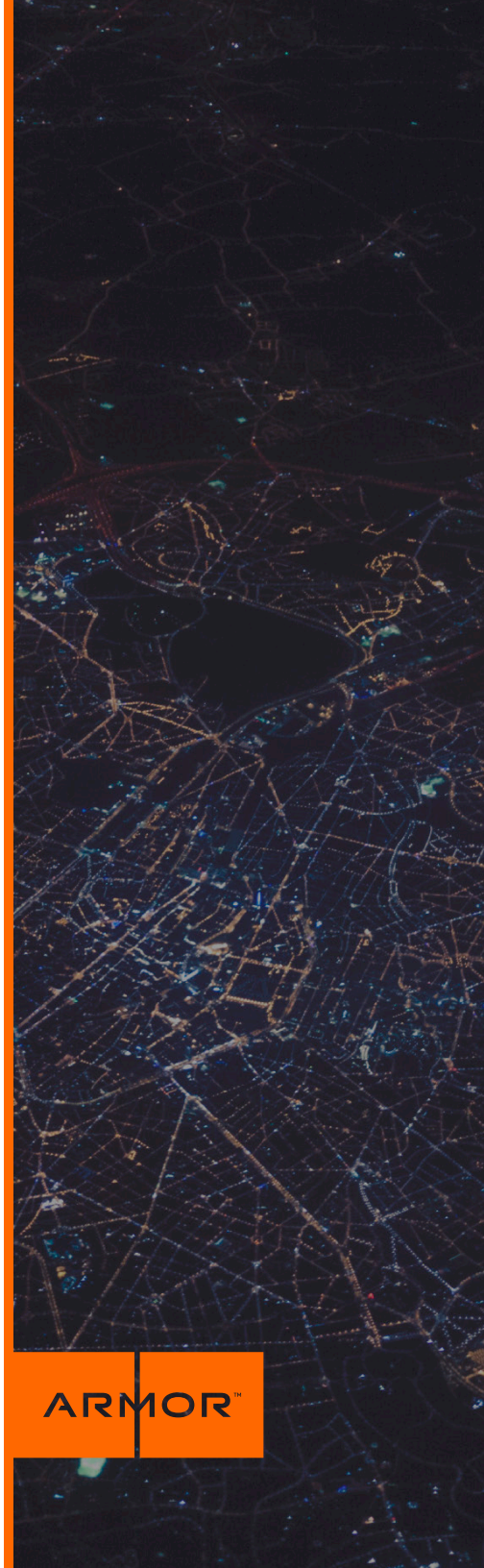
Before you get started on blazing your own path toward cloud security independence, it's important to understand the pitfalls of doing it yourself, especially when it comes to Payment Card Industry Data Security Standard (PCI DSS) compliance.

While more prescriptive than some of the other data compliance standards, such as HIPAA, PCI can still be a moving target for many organizations that handle payment card data. It's continuous evolution, now current up to DSS 3.2, only adds to the difficulty. Without a clear understanding of its nuances, even the most state-of-the-art solution won't make it past an annual compliance audit.

Despite the challenges, having complete control of your IT environment is an advantage you may decide is worth the risk.

This white paper is intended to serve as a detailed guide for those pursuing PCI DSS compliance on their DIY cloud security environment.

Without a clear understanding of its nuances, even the most state-of-the-art solution won't make it past an annual compliance audit.



Basics for builders

First, let's start with the basics.

It should come as no surprise that companies planning to build their own cloud security solution need to have an understanding of the current PCI DSS, the expertise to manage the cloud environment and knowledge of the PCI Standards Council's Cloud Computing Guidelines. Additionally, compensating controls must be in place.

Gaining clarity on which services are relevant to an organization's transmission, processing, and storage of cardholder data is a significant effort in itself.

A customer needs to investigate which technologies and systems are used by the cloud hosting provider, which third-party vendors are involved in the data loop, and which core processes are housed in the host's facilities that may touch the customer's services. Inventories of all these systems have to be kept up-to-date, and changes may require a review of a customer's current security measures to be sure they stay up to date.

Nearly 80%

of all businesses fail their interim PCI compliance assessment.

Source: 2015 PCI Compliance Report, Verizon Communications.

Compensating Controls

A compensating control provides a workaround when a PCI requirement cannot be met for physical or technical reasons. The mandatory Compensating Control Worksheet (CCW) contains seven areas that must be addressed.

PCI DSS Updates

PCI 3.2

COMPLIANCE

The latest version of PCI DSS requires a change management process to be in place to accommodate continuous monitoring of the environment. In the previous version, only a yearly assessment was mandated.

In addition, pen tests must be conducted every six months instead of every year. These should be scheduled with a cloud hosting provider.

The boundaries of responsibility

Now, with the 'what' and the 'how' covered, let's talk about the 'who.' Specifically, who will be responsible for the various aspects of PCI compliance on your public cloud environment.

Determining which party is responsible for PCI compliance in the cloud can be murky. The host is responsible for some pieces, the customer for others, and yet others are shared. The customer, you, is responsible for meeting PCI requirements on both its own components and the shared components, and if anything slips through the gaps, you'll be the one held responsible.

Even when running a cloud on a gold-standard service such as Amazon Web Services or Microsoft Azure, responsibility for every aspect of your environment's PCI compliance remains with the customer; that includes service configurations, guest operating systems, and security controls such as intrusion detection systems, anti-virus software, and other tools and software.

Fortunately, most cloud hosting providers will supply a responsibility matrix that covers all twelve PCI requirements. This should be a detailed document that clearly states which organization is responsible for what. For instance, the provider may provide a firewall, while the customer may be responsible for developing firewall rules, testing the network, and implementing segmentation. Unless a customer's assessor attests that some requirements don't apply, the customer is contractually obligated to meet all PCI requirements on its part of the system.

What is a Responsibility Matrix?

Armor Security Services	Armor Complete (Virtual Private Cloud)	Armor Anywhere (CORE)	PCI DSS 3.0 Controls	HIPAA/HITECH Controls	Risk Mitigation
PERIMETER LAYER					
IP Reputation Filtering	☑		Security best practice	Security best practice – implied control under 164.306(A)	Activity from known bad sources
DDoS Mitigation	☑		Security best practice	Security best practice – implied control under 164.306(A)	Loss of availability due to high volume of malicious activity
APPLICATION LAYER					
Web Application Firewall	☑		6.6	Security best practice – implied control under 164.306(A)	Application layer flaws and exploits
NETWORK LAYER					
Intrusion Detection	☑		11.4	Security best practice – implied control under 164.306(A)	Malicious allowed traffic
Network Firewall (Hypervisor-Based)	☑		1.1.4, 1.1.5, 1.2.2, 1.2.3, 1.3.4, 1.3.6	Security best practice – implied control under 164.306(A)	Unwanted network connectivity
Internal Network Vulnerability Scanning	☑		11.2.3		Exploits due to missing patches/updates; improper network firewall configuration
External Network Vulnerability Scanning	☑		11.2.2	Security best practice – implied control under 164.306(A)	Exploits due to missing patches/updates; improper network firewall configuration
Secure Remote Access (Two-factor authentication)	☑		8.3	§164.312(d), §164.312(a)(2)(iii)	Unauthorized remote use of administrative access
Encryption in Transit (Armor SSL certificates only)	☑		4.1.c, 4.1.d	§164.312(e)(1)	Interception of sensitive data in transit

Armor's responsibility matrix is a document that defines which areas of an environment are the responsibility of the host and which are the responsibility of the customer.

Questions to ask a cloud hosting provider

Q | What parts of the twelve PCI standards are the host's responsibility, which are shared, and which are yours?

A | Study the host's responsibility matrix carefully and identify any areas that are not clearly assigned.

Q | Does the host have enough staff who fully understand PCI DSS security? What is the proof of their ability?

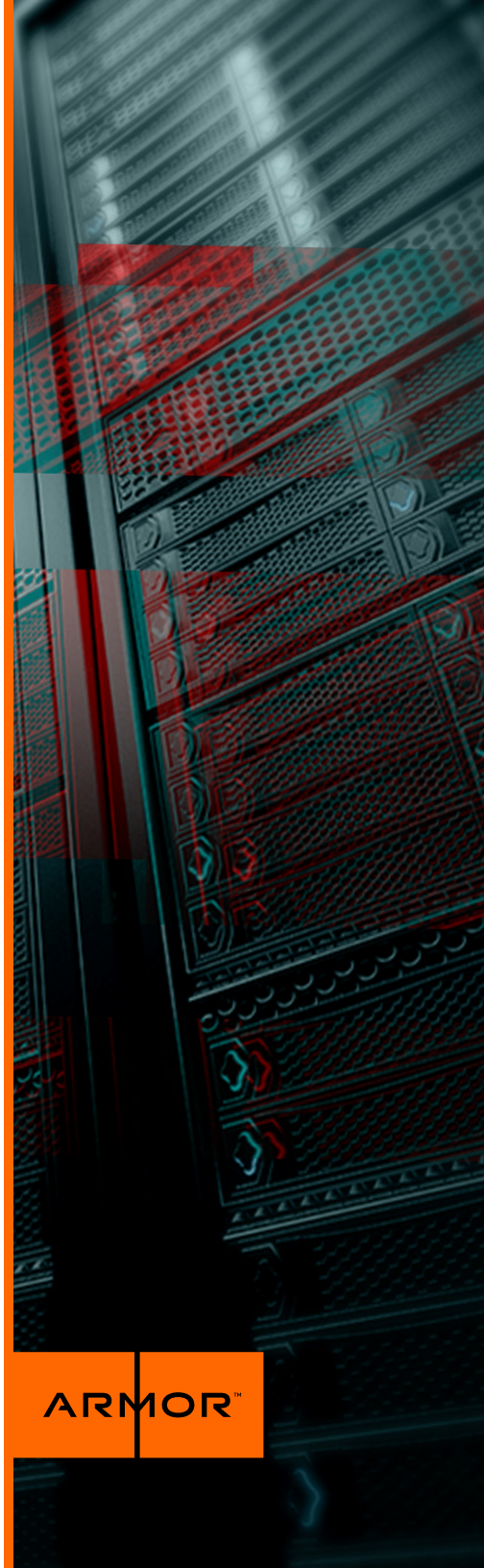
A | Certifications are not enough; the host's security analysts should have real-world experience working with organizations similar to yours. Even their less experienced staff members should have been trained on handling PCI-covered data because human error is the cause of many breaches.

Q | Is the host continuously monitoring systems around the clock?

A | The answer must be more detailed than a simple yes. The NIST standard describes 'continuous monitoring' as "assessed, analyzed and reported at a frequency sufficient to support risk-based security decisions." What is that frequency? Are you satisfied with it?

Q | Does the host monitor bandwidth to detect Denial of Service attacks?

A | The worst ways to discover a Denial of Service attack is to receive a bill for magnitudes of gigabytes greater than you typically use, or to get calls from customers saying they can't access their accounts. Cloud hosting providers are a popular target for DoS attacks since attackers can use the DoS to conceal other malicious activities and escape with sensitive data from many companies at once. Ask your host to describe the tools and policies they have in place to identify attacks promptly.



Questions to ask a cloud hosting provider

Q | How quickly can they respond to an attack?

A | Your host should respond immediately, but remediation times will depend on variables that can't be predicted. The host should, however, have a plan to add bandwidth, scrub bad traffic, and take other specific steps to reduce the impact of an attack. These should be documented and shared with you.

Q | How quickly will you be notified of an attack?

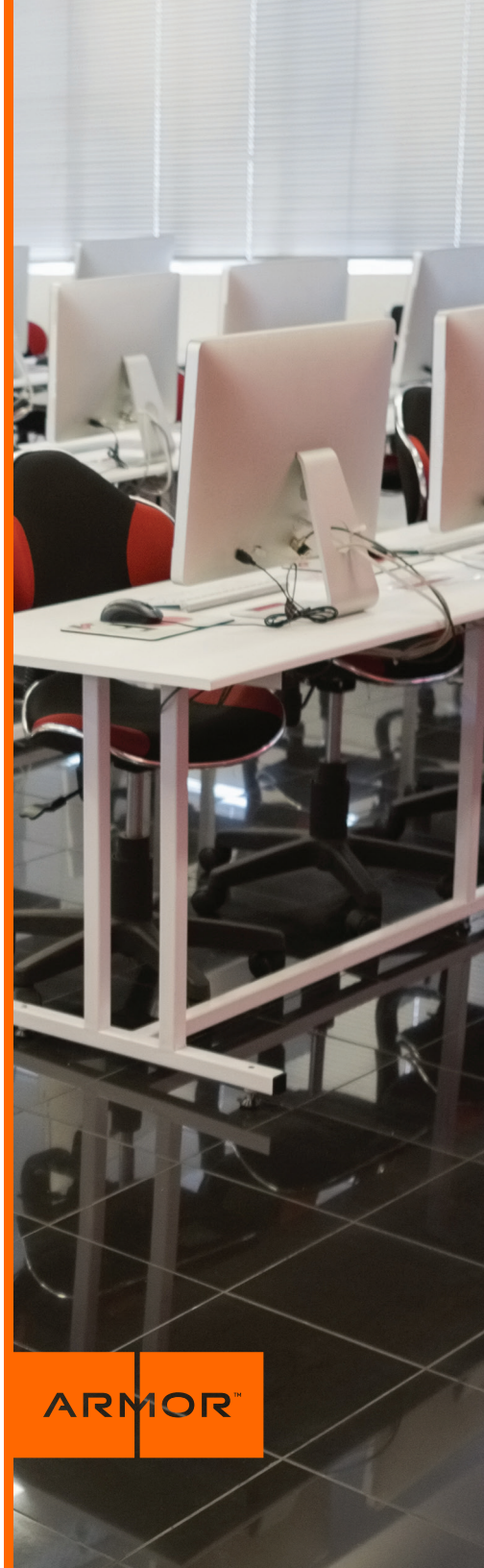
A | As soon as the provider becomes aware that an attack is in progress.

Q | Will the host help you if you are breached?

A | Specific actions should be detailed in the service level agreement.

Q | Does the hosting package include firewalls, vulnerability scanning, file integrity monitoring, daily log review, and backup/disaster recovery?

A | Some services may be provided at additional costs.



Your technical responsibilities

The technical requirements to implement PCI security on a cloud-hosted environment are lengthy; for example, the Responsibility Matrix for Google Cloud Platform is 55 pages long. Expect to perform security activities in the following general areas:

Install and maintain a dedicated cloud firewall configuration to protect cardholder data.

A dedicated cloud firewall is stateful so it can keep a record of interactions. It may offer other security functions as well, such as intrusion prevention.

Manage passwords, keys, and encryption.

Additional encryption will be required for cardholder data stored on instances' encrypted volumes. Do not use the default passwords or other security parameters that come with vendor-supplied tools; hosts will require these to be changed and managed.

Identify and access management is the customer's responsibility.

That includes restricting physical access to data, documenting and enforcing data access policies, and ensuring that password policies are in line with the provider's. Third-party tools will almost certainly be required in order to administer the host's directory service.

Encrypt transmission of cardholder data across open public networks.

This may require the use of elastic load balancers, network ACLs, customer gateways, virtual private gateways and other tools that will have to be configured, patched, tested and upgraded by the customer

All systems will have to be protected by antivirus software that the customer maintains and updates.

Scanning, logging, and reporting will be the customer's responsibility.

A host is not likely to provide systems that directly address PCI requirements for software development and change control.

Third-party vulnerability and patch management solutions must be installed and maintained.

The customer must track and monitor all access to its systems and cardholder data.

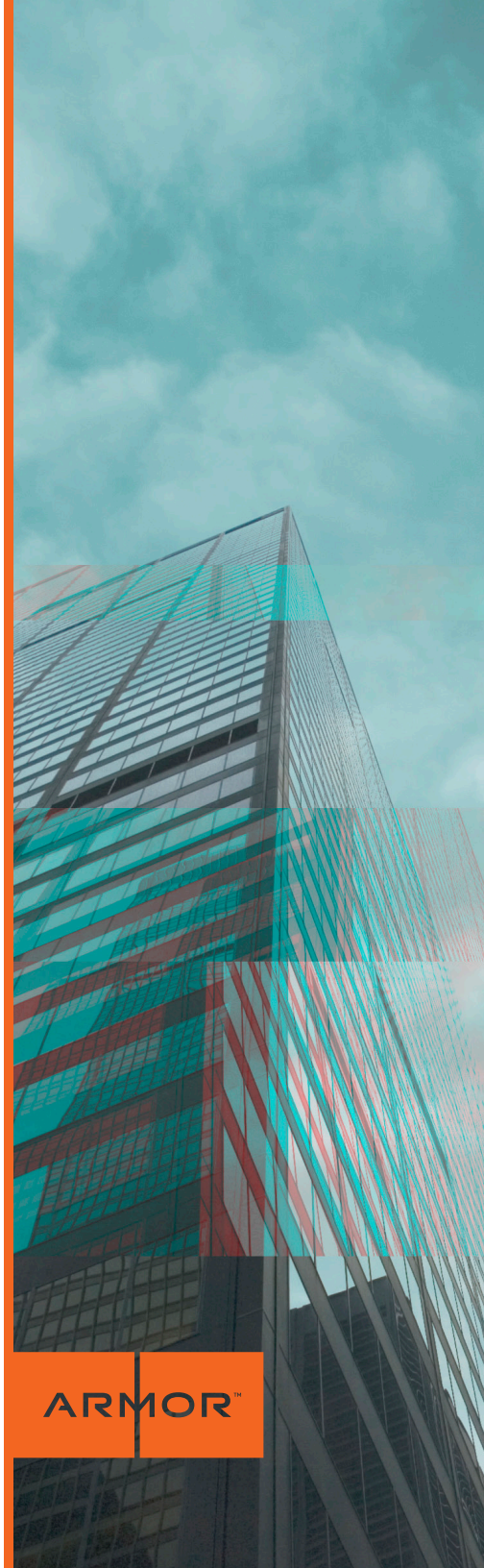
Activity may be relatively straightforward if a customer is using a Security Information and Event Management (SIEM) solution has an API that works with its cloud hosting provider's solution. Otherwise, the customer will have to work with its SIEM vendor and cloud hosting provider to connect the systems.

Testing in the forms of vulnerability scanning, penetration testing, intrusion prevention, and file change detection are likely to be the customer's responsibility.

An array of third-party solutions will be needed to handle these services, but be aware that most tests must be scheduled with the cloud hosting provider beforehand.

Cloud hosting providers will not be able to provide information security policies for a customer's organization.

The customer will need to create that documentation on its own or engage a third-party vendor to assist with the effort.



Trust and Security

No matter how you decide to approach security on your public cloud environment, compliance is only one aspect, albeit a critical one, for determining effectiveness. At the end of the day, your customers trust in you to protect their data from internal and external threats.

Any solution will have to provide this level of assurance.

While cloud security independence can be alluring to some organizations, most will struggle when required to divert IT resources from their core business to maintain daily monitoring and scanning.

Luckily you don't have to go it alone.

A cloud security vendor that has repeatedly implemented PCI compliance should be aware of the pitfalls a particular customer is likely to encounter during its implementation. They will own, maintain and upgrade the necessary security tools, as well as handle scanning, testing and logging without the need for any special action on the customer's part. Audits are simplified because a cloud security provider's design strategy will be custom-built to meet the specific needs of PCI DSS-driven companies.

They should have an infrastructure that decouples the larger IT environment and the world at large from critical payment data, separating the two with multiple layers of managed security.

Network topology is critical, but human capital is just as important. Look for a provider with intelligence specialists on staff who are capable of forecasting attack trends and taking proactive measures to deter attackers, as well as ethical hackers who constantly test the systems for vulnerabilities and experienced security professionals who can provide advice and guidance to help customers meet their security and compliance goals.

Here when you need us

Cloud security is tough. We would know. At Armor, it's something we've learned from experience.

Every cyber attack, audit and bit of customer feedback acts as a data point to help us further improve our services and solutions. Meaning, that we are only getting better at keeping threat actors out and compliance auditors happy.

We've navigated these intricacies ourselves, so whether it's the monitoring and analysis of day-to-day security operations or helping prepare for annual PCI audits, we know what it takes.

So, try on DIY security for yourself, but be rest assured that we're here if you ever need us to help share the burden of security and compliance.

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167