Ensuring PCI DSS Compliance in the Cloud

A simple approach based on ownership control and shared responsibility can help organizations more effectively migrate PCI DSS compliance to Amazon Web Services’ public cloud.

Executive Summary

The adoption of public cloud services has proven effective across a diverse set of industries, as numerous successful use cases illustrate. Regardless of its many operational and cost benefits, however, organizations need to think about the cloud’s security implications and how the model will also affect data privacy and availability.

Decisions get further complicated once a cloud services provider enters the picture. Organizations that must ensure the security of cardholder data, for example, often find the challenge of complying with the Payment Card Industry Data Security Standard (PCI DSS) difficult and overwhelming. This standard is defined by a structure of 12 requirements to ensure the security of cardholder data that is stored, processed and/or transmitted by merchants and other establishments.

Given its comprehensive nature and the surfeit of information on security procedures and requirements, personnel responsible for ensuring the security of cardholder data are often at a loss on where to start and how to go about establishing compliance.

This white paper offers a simple and time-tested approach based on ownership control that can help IT organizations, merchants – their customers – and other stakeholders to incrementally mitigate the risk factors on their path toward achieving PCI DSS compliance. The paper provides an overview of cloud components, compliance requirements, challenges in ensuring compliance, cloud security best practices and how our approach can help to determine which parties are responsible for what security mechanisms and how doing this can more effectively resolve customer issues.

This white paper highlights our approach to compliance from an Amazon Web Services (AWS) infrastructure as a platform (IaaS) environment perspective, and it highlights the benefits of this approach for companies seeking to achieve PCI DSS compliance using AWS.

The Cloud, So Far

Cloud adoption is growing at a rapid rate, assisted by technological advancements such as high-speed Internet connectivity and innovations in systems hardware. These advancements have brought down the costs of compute and data storage and enabled service providers to meet and, in some cases, exceed customer expectations in terms of scalability, availability and cost. But this in turn has introduced new complications concerning user security considerations. User companies must clearly understand the scope of responsibility that the cloud service provider accepts for each PCI DSS requirement, and which
services and system components are validated for each requirement. The areas of responsibility and accountability vary for every service and deployment model.

Before detailing this, it is important to understand the three cloud service models and cloud deployment models. These service and deployment models are relevant to our approach based on ownership control in determining which parties are responsible for what security (see sidebar).

Cloud service models include:

- **Infrastructure as a Service:** In the IaaS model, the cloud provider gives the customer the capability to provision storage, processing, networks and basic computing resources in which the customer can deploy and run any arbitrary software, including operating systems and applications. The cloud provider manages and controls the underlying cloud infrastructure; the customer only controls the storage, operating systems and deployed applications.

- **Platform as a Service:** In the PaaS model, the cloud provider gives the customer the capability to deploy onto cloud infrastructure custom/acquired applications developed using programming languages, libraries, tools and services supported by the cloud provider. The cloud provider controls and manages the underlying cloud infrastructure, along with the network, operating systems, storage and servers; the customer retains control over the deployed applications and usually the configuration settings for the application hosting environment.

- **Software as a Service:** With SaaS, the cloud provider offers the customer the capability of using applications running on its cloud infrastructure. These applications can be accessed from various client devices such as a Web browser or a program interface. The cloud provider manages and controls the underlying cloud infrastructure, along with the network, operating system, servers, storage and individual applications, except for a few specific application configuration settings.

---

**Quick Take**

### Have It Your Way

The way customers deploy services from cloud providers falls into one of the following three models:

- **Public:** This type of cloud infrastructure model is open to the public at large. The service organization typically owns, manages and operates the service from its own premises.

- **Virtual private cloud:** This type of cloud infrastructure is solely for a single organization. It is either managed by the organization or a third party, and may be located either on-premises or off-premises.

- **Hybrid:** In this type, the cloud infrastructure comprises two or more clouds that are either private, public or community clouds that remain as unique entities but are bound by the standardized technology.
Challenges in Cloud PCI Compliance

The path to PCI DSS compliance is complicated, but it must be addressed by all businesses dealing with storing, processing or transmitting cardholder data. And it is often a daunting responsibility for IT teams to ensure compliance with all 12 PCI DSS requirements, along with 100-plus security controls.

First, large organizations including banks, retail chains and e-commerce companies with exceedingly large cardholder data environments have greater difficulty fully complying with PCI DSS. This is because the PCI standards require changes to be made at all levels, from infrastructure to operating system to network level, and so on. The distributed-layer architectures of cloud environments add layers of technology and complexity to the exercise.

Another challenge is that though PCI DSS is perceived as a business enabler in some organizations, many others see it as a hindrance and a necessary evil that must be dealt with only when absolutely necessary. This perception can translate into fines, penalties and needless sanctions levied when organizations fail to comply.

Public clouds are designed to allow access into the environment from anywhere on the Internet. Hence, additional controls must be employed to compensate for the inherent risks and lack of visibility into the public cloud architecture. These challenges may make it difficult and in some cases impossible for public-cloud-based services to operate in a PCI DSS-compliant manner. Therefore, the burden for providing proof of PCI DSS compliance for a cloud-based service falls on the cloud provider, and customers should accept such proof only after checking evidence of appropriate controls.

Thus, it is imperative for companies to get sufficient assurance that the scope of the provider’s PCI DSS review is sufficient, and that all controls applicable to the hosted entity’s environment have been evaluated and determined to be PCI DSS compliant. The cloud provider should also be prepared to provide its hosted customers with evidence that clearly indicates what was or was not included in the scope of its PCI DSS assessment. Controls that were not covered are therefore the customer’s responsibility in its own assessment. The cloud provider should also provide the details of which PCI DSS requirements were reviewed and considered to be in place and not in place – as well as confirmation of when the assessment was conducted.

Any aspect of the cloud-based service that is not covered by the cloud provider’s review should be identified and documented in a written agreement.
Any aspect of the cloud-based service that is not covered by the cloud provider’s review should be identified and documented in a written agreement. The hosted entity should be fully aware of all aspects of the cloud service, including specific system components and security controls, that are not covered by the provider. These then should be managed and assessed by the hosted entity itself.

It makes more sense to get assistance from a PCI-compliant managed services provider. The rewards of this are clear and valuable: they require no capital expenditure by the user organization, offload significant demands from internal IT staff and expedite PCI compliance validation. Moreover, they help organizations avoid hefty fines and financial penalties.

Cloud Security: An Evolving Capability

Figure 2 illustrates at a high level how control is assigned between the customer and cloud service provider in the three cloud service delivery models.

The various roles and responsibilities for security vary across the different cloud service models. To address the various security needs of the workloads or cloud scenarios, organizations need to understand the ownership responsibilities for protecting these workloads. The responsibility for security increases for the cloud service provider at higher levels of the stack and increases for the user organization at lower levels.

In an IaaS model, for example, the cloud provider is responsible for the security of just the infrastructure, but in the SaaS model the cloud provider is responsible for the security of both the infrastructure and the application.

The sidebar on page 5 offers a brief description of various PCI compliance requirements and how they can be addressed in AWS.

PCI Compliance Requirements: An Overview

As Figure 3 (next page) shows, PCI DSS compliance requirements can be classified into six security domains. This breakdown can help in mapping security best practices recommended on public IaaS environments such as AWS.

Using this classification, we can further map each security requirement to IaaS provider and user organization responsibilities. This classification will help user organizations understand security best practices on AWS and help them determine their coverage in meeting and maintaining the compliance requirements.
**Cloud Security and Compliance Approach**

**Network Security**

Network security defines the requirements for protecting cardholder data through firewall configurations at the network layer and ensures that system default passwords are changed at the OS platform level. These requirements, at a very high level, can be mapped with the user organization’s responsibility in the AWS IaaS environment and can be achieved through the following security best practices.

**Network Isolation**

AWS offers the ability to define a virtual network dedicated and isolated from other organizations/tenants on the public cloud. This ability to define a virtual private cloud enables organizations to configure a network environment that is very similar to an on-premises traditional network. This environment also allows a virtual private network (VPN) connection to be established between the organization’s on-premises network and the virtual private cloud.

The AWS virtual private cloud allows network configuration that is very similar to a typical Web application deployment environment. This environment has a public subnet, or demilitarized zone, hosting Web servers and private subnets hosting applications, as well as database servers.

**Compliance Requirements Classification**

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security</td>
<td>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</td>
</tr>
<tr>
<td></td>
<td>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Requirement 3: Protect stored cardholder data.</td>
</tr>
<tr>
<td></td>
<td>Requirement 4: Encrypt transmission of cardholder data across open, public networks.</td>
</tr>
<tr>
<td></td>
<td>Requirement A.1: Shared hosting providers must protect the cardholder data environment.</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Requirement 5: Use and regularly update anti-virus software or programs.</td>
</tr>
<tr>
<td>Program Data Protection</td>
<td>Requirement 6: Develop and maintain secure systems and applications.</td>
</tr>
<tr>
<td>Access Control Measures</td>
<td>Requirement 7: Restrict access to cardholder data by business need to know.</td>
</tr>
<tr>
<td></td>
<td>Requirement 8: Assign a unique ID to each person with computer access.</td>
</tr>
<tr>
<td></td>
<td>Requirement 9: Restrict physical access to cardholder data.</td>
</tr>
<tr>
<td>Monitor and Test Networks</td>
<td>Requirement 10: Track and monitor all access to network resources and cardholder data.</td>
</tr>
<tr>
<td></td>
<td>Requirement 12: Maintain a policy that addresses information security for all personnel.</td>
</tr>
</tbody>
</table>

---

*Quick Take*

Amazon’s Approach to PCI DSS Compliance

AWS is PCI DSS Level 1 compliant. This means that organizations using the AWS IaaS can rely on the PCI Compliance Validation of the technology infrastructure while managing compliance and certification of their own environment. AWS service provider compliance covers all requirements as defined by the PCI DSS for physical infrastructure service providers.

AWS recommends a shared responsibility model for organizations hosting their applications on its infrastructure. In this model, AWS is responsible for physical and virtual infrastructure up to the level of virtual machine (hypervisor) and the organization is responsible for operating systems (OS), firewalls, antivirus, middleware, applications and account management. AWS supports this approach with various security best practices that are applicable to organizations in achieving and maintaining PCI compliance on an ongoing basis.

---

*Figure 3*
Private subnets can be configured with various inbound and outbound rules that meet the exact requirements of the hosted applications, including monitoring and management.

Software Firewalls
Firewall configurations at the individual server level provide the ability to block access from hosts outside the specified subnets. Firewall configurations on AWS environments can be created to meet the existing firewall configuration rules on on-premises networks. This ability to administer firewall configurations and maintain audit logs pertaining to changes in the configuration is a key requirement of PCI DSS compliance. AWS security groups/firewall configurations for servers also produce audit logs of changes to configurations by administrators.

Data Protection
Data protection defines the requirement of guarding cardholder data during both storage and transmission of data across open, public networks. These requirements can be addressed by user organizations in AWS through the following security best practices for encrypting data at rest and in transit.

Transport Layer Security through SSL
Applications designed to handle or transmit cardholder data use SSL for securing the Web request/responses. SSL termination is usually handled by Web/app servers that can be off-loaded to load balancers on AWS environments. Off-loading the SSL termination from Web/app servers ensures that the keys are not stored on individual instances and are stored within secure cloud storage locations that can be protected through permissions.

Key Management Interface
Applications designed for PCI DSS compliance require encryption based on public-key cryptography or the Advanced Encryption Standard. These encryption technologies depend on secure key management systems that are certified for PCI DSS compliance. Key management systems, such as the cloud hardware security modules that are available as appliances on the AWS environment, can be used for this purpose. This dedicated appliance provides a secure key storage and a set of cryptographic operations for encrypting and decrypting data. The appliance can be hosted on a private subnet and can only be accessed from secure instances within the subnet by administrators/users with specific roles.

Secure Cloud Storage
Applications designed for storage of cardholder data will need to encrypt data stored in the file or database storage locations. AWS supports data encryption at the time of storage automatically through transparent data encryption and native network encryption enabled on the AWS relational data services. AWS Cloud Storage S3 also offers encryption of data using both client- and server-side encryption. This ensures that data can be encrypted during storage and cannot be accessed directly.

Vulnerability Management Program
Vulnerability management defines the requirement for building and maintaining an environment that has anti-virus technology installed.
and updated regularly; file integrity monitoring enabled at the system level; intrusion detection and prevention at the network level; and avoidance of common vulnerabilities at the application and database implementation level. AWS supports various third-party security SaaS providers that offer network intrusion detection and prevention capabilities. The following security best practices details the approaches involved in incorporating these solutions.

Anti-Virus Installation

PCI DSS specifies that the OS platforms are installed with anti-virus software and updated on a regular basis by automated virus definition updates. The golden images prepared in AWS can be installed with anti-virus software and configured to allow periodic downloads from anti-virus virus definition and software updates. As the server instances are usually hosted on private subnets, these subnets are configured with network address translation server (NATS) instances to allow outbound Internet access for these updates.

Configuration Management

PCI DSS specifies that the server instances need to be monitored for any drift/change in configuration and logged as an event that can be used for alerting the system administrators or IT management. The configuration manager also needs to produce daily reports that can be analyzed by the security team for any tampering of the configuration on these instances. These reports are to be stored and later archived for a specified time period.

This can be approached by configuring file integrity monitoring enabled on all server instances to monitor critical configuration files. This monitoring is enabled through a system level intrusion detection environment that is capable of alerting administrators via e-mail whenever any configuration change takes place. The configuration varies based on the server type, as the directories to be monitored for the Web server are different from app or database servers.

Network Intrusion Detection and Prevention Systems

PCI DSS specifies the network intrusion detection and prevention systems used for monitoring network traffic to stop various threats on an ongoing basis. These systems are required to execute various vulnerability scans to ensure that the systems are compliant on a daily basis and produce detailed vulnerability reports of the various hosts in the network. Third-party vendors offering intrusion detection and prevention systems also support PCI DSS compliance and are approved by the PCI Security Standards Council.

Configuring a third-party intrusion detection and prevention offering via an SaaS delivered model is supported by the AWS cloud. IDS/IPS launches an appliance/agent on the public subnet of the cloud environment that is capable of monitoring network traffic and conducting scans of the hosts in the specified network. IDS/IPS is updated by vendors on a regular basis to continuously detect upcoming or emerging threats.

AWS supports various agent-/appliance-based monitoring of virtual private cloud environments supporting compliance requirements.

Application Vulnerabilities

PCI DSS specifies that application/database design and implementation need to eliminate common risks/vulnerabilities as defined by the Open Web Application Security Project (OWASP) top 10 and SANS Institute Common Weakness Enumeration (ICWE) top 25. The application and database security needs to address these risks/vulnerabilities through various security best practices that are applicable to both on-premises and cloud deployment environments. Following are some of the common best practices applicable to Web applications:

- **Authentication and authorization:** The application needs to implement best practices on authentication and session validation for user requests. Invalid login attempts are tracked by the application; user accounts are then automatically locked. The application validates the user session on every request and allows access only to authorized pages on the application.

- **Rate limiting and CAPTCHA implementation:** The application needs to implement rate limiting based on the client IP address and does not allow any user to send more than a specified number of requests per second. This ensures that any automated attack on the Web application is blocked by filter mechanisms. The application can use CAPTCHA on critical functionalities such as handling user registrations and capturing payment information. This ensures that any automated attack on the critical functionality is prevented.
• **Web container filters:** The application needs to implement filters to screen all input fields for SQL and OS command injections. This ensures that any attempts to inject scripts through input fields are blocked. Uploading of scripts through HTTP commands is blocked by Web server configurations. The application also uses standard libraries available as part of the Web container to block cross-site request forgery.

Common weaknesses include several other software errors that can be addressed through application design, Web frameworks and container-based mechanisms. All are common across on-premises and cloud environments.

**Access Control Measures**

An access control measure defines the requirement for restricting access to data to various user groups and roles across production and development/test environments. This also requires that users are uniquely identified and their actions can be logged for auditing purposes. This requirement also defines the various restrictions on physical access to cardholder data through access to physical infrastructure. AWS provides identity and access management that can be structured to meet the access control requirements across environments. As the physical infrastructure is under the control of AWS, this requirement is primarily addressed by PCI compliance measures adopted by AWS.

**Cloud Identity and Access Management**

PCI DSS specifies various access rules for authorized personnel accessing the systems at physical infrastructure level and as system administrators. IaaS providers typically ensure compliance of PCI DSS at the physical infrastructure level and require IaaS account management to be performed by users at the organizations. PCI DSS requires the identity and access management of IaaS providers to enable multifactor authentication and role-based policies for administrators and developers.

This can be approached by specifying administrator and developer role policies to restrict access to various environments such as development, testing, staging and production. These policies prevent unauthorized users from accessing restricted environments containing sensitive cardholder data. This ensures that critical systems such as Keystore, database and virtual private cloud (VPC) environments are inaccessible to unauthorized personnel. These policies are also extended to API-based access to AWS environments. This will ensure that unauthorized personnel do not programmatically access these critical resources on the cloud environment. Administrators are also required to use multifactor authentication to access the AWS management console, which is a critical requirement specified by PCI DSS.

**Monitor and Test Networks**

Monitor and test networks define the requirement for monitoring access to the network and data. This requires enabling various application level access and administrative activities, which can be later analyzed for any unauthorized accesses (with notifications sent to authorized personnel). This also requires that various vulnerability and penetration tests are carried out on an ongoing basis to detect any noncompliance due to configuration changes. AWS provides audit logging mechanisms for administrative activities. The application environments can also be enabled to generate logs that can be later aggregated and analyzed in the cloud environment. This environment also allows penetration and vulnerability scans by third-party SaaS providers with advance notification to AWS.

**Cloud Administration: Audit Logging**

PCI DSS specifies that all administrative access to deployment environments should have audit logging enabled, which can be verified during audits. IaaS providers support the logging of various administrative activities performed in the cloud environments either through the console or APIs. AWS Cloud Trail provides an activity log that requires further processing to extract relevant activities.

Our Trail Digest is an appliance for AWS that is capable of processing audit trails logged by AWS and generating relevant reports and notifications for certain specified events. The real-time monitoring of administrative access logs is critical in ensuring that configuration changes do not affect PCI DSS compliance and do not lead to a security breach. All critical configurations such as software firewalls, VPC rules and launching/termination of server instances are monitored near real time and alerted through notifications to authorized personnel.

**Cloud Audit: Automated Verification**

PCI DSS specifies the monitoring and verification of deployment environments on a regular basis to ensure compliance. This requires the verifica-
tion of the environment both through manual or automated processes to ensure that any ongoing changes in the environment do not lead to any violation of compliance requirements.

Our Audit Equip is an automated compliance verification tool built for cloud IaaS and PaaS environments. This tool is an AWS-based solution that has encoded the PCI compliance rules and is capable of verifying the deployment environment for any violations of the rules. This tool also supports manual verification through a questionnaire that provides the necessary checklist for audit teams. This tool supports the PCI requirement of continuous monitoring and validation of the AWS environments.

Security Monitoring: Log Aggregation and Analysis
PCI DSS specifies the logs generated by Web, app and database servers; user access logs must be stored securely and available for audit purposes.

This can be approached by configuring log aggregation and analysis solutions deployed as an appliance on AWS environments. The server instances running Web, app or database servers generate logs that can be rotated periodically to secure the cloud storage location, which is accessible to these log analysis systems. The server instances can also be enabled with system level intrusion detection that generates daily logs of activity. All individual logs are aggregated on cloud storage and then analyzed for security requirements.

Information Security Policy
Organizations and PCI-compliant IaaS providers must update their information security policy based on the shared responsibility model. This process requires understanding the PCI compliance achieved by the IaaS provider for the technology infrastructure and for the organization's information security policy covering PCI compliance on the OS, middleware and application layers.

Looking Forward
There are numerous ways to leverage the advantages of cloud-based models for PCI DSS compliance, but it is also necessary for enterprise IT organizations to be aware of and responsible for various aspects of security. While this task is often seen as daunting, it should not discourage organizations from moving to the cloud. All that the organization needs is to understand the responsibilities in their shared responsibility model and adopt the best practices similar to what is outlined in this white paper to ensure PCI DSS compliance.

This white paper outlines our viewpoint and some of the best practices by which end-user organizations can ensure PCI DSS compliance. But these are the first steps to becoming PCI compliant. In order to remain PCI compliant, processes need to be in place and refined throughout the year. The key to ensure ongoing PCI compliance is continuity.

• Make someone accountable and responsible. Give someone responsibility for ascertaining that all IT and business processes ensure the PCI DSS compliance requirements.

• Configuration control is the key. Configuration management is all about ensuring that the right versions are in the right places.

• Have a vulnerability management system in place. Ensure that all vulnerabilities are addressed, including less important ones.

• Establish patch management and change control: Orchestrate or automate your patch management and make it a continuous process. Patch management should be carried out within a change control framework.
References


About the Authors

Srikarthik Venkataraman is a Senior Architect within Cognizant’s Cloud Practice. He focuses on architecting application migration to the cloud with an eye toward security and compliance requirements. Srikarthik previously architected SaaS-based solutions for various analytics platforms in the areas of speech to text conversion and social media monitoring. He holds a B.E. degree from Madras University and is currently working on his master’s in software engineering at BITS, Pilani. He can be reached at Venkataraman.Srikarthik@cognizant.com | LinkedIn: www.linkedin.com/in/srikarthikv.

Arjun Anand is a Business Development Manager within Cognizant’s Cloud Services Business Unit. In this role, he is responsible for building cloud solutions/assets, supporting the company’s cloud strategy and execution across industry domains and assisting in cloud consulting engagements. Arjun has rich experience in the software industry in the areas of global delivery and has held various program and project management roles on numerous application development and outsourcing initiatives. He is also a Certified Scrum Master (CSM). Arjun holds a B.E. degree from Anna University and a PGDM from Indian Institute of Management (IIM), Bangalore. He can be reached at ArjunAnand.D@cognizant.com | LinkedIn: http://www.linkedin.com/in/iimbarjun.

About Cognizant Cloud Services

Cognizant Cloud Services works closely with Amazon Web Services (AWS) to deliver flexible, elastic and scalable security solutions that are compatible with the AWS environment. We also understand that in order to resolve all the security challenges, no compromises should be made on the cloud’s operational and economic benefits. As such, we help organizations embrace the cloud by devising strategies to overcome the perceived security concerns as they look to migrate their applications to a cloud environment.

We deliver the broad range of security capabilities as part of the shared responsibility model, including packaged solutions and blueprints in place to help ease the customer’s path to compliance. For instance, our PCI DSS compliance-ready environment can be used to migrate any PCI DSS application to the cloud. With this blueprint, customers could host their PCI-compliant application on an AWS public cloud and assess how PCI DSS compliance would be fulfilled.

To find out more about Cognizant’s cloud solutions, please visit: www.cognizant.com/cloud-computing or www.cognizant.com/businesscloud.
About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world’s leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 75 development and delivery centers worldwide and approximately 178,600 employees as of March 31, 2014, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.