**AWS PCI DSS**

PCI DSS is a cybersecurity standard backed by all the major credit card and payment processing companies that aim to keep credit and debit card numbers safe. PCI DSS stands for ​Payment Card Industry Data Security Standard. The standard, which is administered by the Payment Card Industry Security Standards Council, establishes cybersecurity controls and business practices that any company that accepts credit card payments must implement. Companies can demonstrate that they've implemented the standard by meeting the reporting requirements laid out by the standard; those organizations that fail to meet the requirements, or who are found to be in violation of the standard, may be fined.

Credit and debit card numbers are probably the most valuable sequences of digits around: anyone with access to them can immediately make fraudulent purchases and drain money from user accounts. Because banks and other credit card issuers will generally refund their customers in these situations, they have invested interest in ensuring that credit card numbers remain secure as they are transmitted across the economic ecosystem. The PCI Security Standards Council was created by these industry players to make sure that transactions involving credit card numbers are secure as possible. The Council lays down several security standards that organizations in different industry segments must implement for instance, PCI PTS covers manufacturers of PIN-based devices, and PCI PA-DSS governs software developers writing code that manages cardholder data.

PCI DSS is the most wide-ranging of the Council's standards. It applies to "any entity that stores, processes, and/or transmits cardholder data," which means that any organization that accepts credit card payments which is to say, any virtually any organization that sells anything or accepts donations must adhere to the standard.

You are the cybersecurity analyst for a retailer that is considered a Tier 1 merchant (the highest) under PCI DSS. Your company wants to migrate to the cloud, specifically Amazon Web Services (AWS). However, they aren’t sure how to maintain their PCI compliance once they do that. They know that AWS operates on a Shared Responsibility Model, but they are fuzzy on the details. The link explaining this model is below.

AWS: Shared Responsibility Model

There are twelve requirements within the standard, with each requirement having multiple sub-requirements, so this project is daunting. Given the work involved, they have hired an outside consultant to perform this effort, and he has gone through the first six requirements. However, he has fallen ill, so your boss has asked you to go ahead and research the seventh and eighth requirements.

Requirement 7 is “Restrict access to cardholder data to business need to know” and Requirement 8 is “Assign a unique ID to each person with computer access.”

Your task is to locate the PCI DSS 3.2.1 on AWS Compliance Guide on the AWS web site, go down to Requirements 7 and 8, and look at each sub-point to determine who is responsible for what. Document what AWS is responsible for, what your company is responsible for, and what options exist within AWS (like the AWS Marketplace) to help your company be compliant.

**RESPONSIBILITIES**

* AWS is in charge of maintaining the infrastructure that supports all of the AWS Cloud's services. This is known as "Cloud Security" by AWS. Computing, storage, networking, database, analytics, application services, deployment, and management are all responsibilities of my company.

**AWS marketplace**

* The AWS Compliance Program assists clients in recognizing AWS's comprehensive cloud security and compliance procedures. AWS Compliance Facilitating factors supplement standard programs by connecting governance-focused, audit-friendly service capabilities with proper compliance or audit guidelines. Clients can then create and operate in an AWS security control environment.  
  Certifications and Attestations, Laws, Regulations, and Privacy, and Alignments and Frameworks are the IT standards to which we adhere. A third-party, independent auditor examines compliance certifications and attestations, resulting in a compliance certification, audit report, or attestation. Customers using AWS are still responsible for adhering to applicable compliance rules, regulations, and privacy programs. Alignments and frameworks for compliance involve stated security or compliance criteria for a specific purpose like a specific industry or function.

Diagram, timeline

Description automatically generated

**THE 7TH REQUIREMENT**

* Much of Requirement 7 is addressed by the customer's access management policy and procedures. The AWS Well-Architected Framework was created by Amazon to assist businesses to establish secure, high-performing, resilient, and efficient infrastructure for their applications. The Security Pillar is concerned with information and system security. Important topics include data confidentiality and integrity, identifying and managing who can do what through privilege management, safeguarding systems, and implementing procedures to detect security problems. Best practices include limiting AWS root account use and access, implementing multi-factor authentication for AWS Management Console accounts, and following the principle of least privilege. It is the duty of the user to keep their AWS resources up to date, for example, by using Amazon Web Services Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS 17. To achieve these strict access control needs, organizations could benefit from their IAM footprint, for example. The default "deny-all" setting in AWS IAM satisfies Requirement 7.2.3. Customers can extend access management control into their on-premises environment by using AWS Cognito, Amazon RDS Identity Federation, and IAM Federation services (*Payment card industry data security standard (PCI DSS) 3.2.1 on AWS* 2020).

**THE 8TH REQUIREMENT**

* It is the customer's responsibility to ensure that their AWS IAM Password Policy is configured to enforce a minimum password length of 7 characters, requires at least letters and numbers or non-alphanumeric characters, has a password expiration of 90 days or less, and prevents password reuse of the last 4 or more passwords. A strategy or automated system must also be in place to identify, remove or disable inactive IAM accounts within 90 days. Customers can do this utilizing AWS services, identity federation with an external customer-managed source, or AWS Directory Service. Many of the account and password requirements can be met with these methods. To satisfy Requirement 8.2.1, IAM handles credentials securely by default. AWS advises using IAM Roles to reduce the requirement for separate user accounts and Amazon SNS topics to notify of specific behavior (*Payment card industry data security standard (PCI DSS) 3.2.1 on AWS* 2020).

Reference

*Payment card industry data security standard (PCI DSS) 3.2.1 on AWS*. (2020, April). Retrieved April 18, 2023, from https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf