Notes 1

In this project the main objective is to learn about PCI DSS in relation to AWS compliance, define roles of who is responsible for what in those requirements (#7,#8), and explore what options exist within AWS (like the AWS Marketplace) to help the company be compliant.

To get a better understanding of PCI DSS is to know what each letter stands for. PCI DSS translates to Payment Card Industry Data Security Standard. "The purpose of PCI DSS is to protect cardholder data (CHD) and sensitive authentication data (SAD) from unauthorized access and loss. It is important to note that PCI DSS is not just a technology standard, it also covers people and processes. Security and compliance are important shared responsibilities between AWS and the customer. It is the customer's responsibility to maintain their PCI DSS cardholder data environment (CDE) and scope, and be able to demonstrate compliance of all controls, but customers are not alone in this journey. The use of PCI DSS compliant AWS services can facilitate customer compliance." Here are some pieces of evidence of the overview of PCI DSS from the AWS compliance guide "(n.d.). Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS. AWS. https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf#:~:text=The%20objective%20of%20this%20guide%20is%20to%20provide,implementation%20to%20their%20PCI%20Qualified%20Security%20Assessor%20%28QSA%29." I chose these bits and pieces from the overview that would give a better understanding of the main goal of PCI DSS that allows AWS to function and allows the customer to gain more knowledge of how it all works together.

While reading through the compliance guide and going through requirements 7 and 8 I have found who is responsible for certain actions between the customer and AWS. In requirement 7 according to the guide " (n.d.). Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS. AWS. https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf#:~:text=The%20objective%20of%20this%20guide%20is%20to%20provide,implementation%20to%20their%20PCI%20Qualified%20Security%20Assessor%20%28QSA%29." It states "It is the customer's responsibility to manage their AWS resources, such as through their IAM footprint, to meet these strong access control requirements." that means if something were to happen to their resources its the customers fault not AWS since its the customers responsibility to manage their resources to have strong access control. In requirement 8 what the customer is responsible for is "It is the customer 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, have a password expiration of 90 days or less, and prevents password reuse of the last 4 or more passwords. Customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or "before" the AWS Management Console at the user endpoint. Customers must grant user access using a least-privilege approach with best practices including password requirements and MFA enforced. Customers must establish database engine identities and roles within the database instance by the customer. " While looking through the guide in requirements 7 and 8 it doesn't state what AWS service is responsible for but what they recommend to help customers have a better service and better security. " . Best practices include limiting AWS root account use and access, requiring multi-factor authentication for AWS

Management Console accounts, and implementing the principle of least privilege. . AWS IAM settings include a default “deny-all” that satisfies Requirement 7.2.3. Customers can leverage AWS Cognito, Amazon RDS Identity Federation, and IAM Federation services to extend access management control into the customer’s on-premises environment. AWS recommends using IAM Roles to further limit the need for discrete user accounts, and Amazon SNS topics for notification of particular behavior. Customers can provide access to AWS resources through identity federation, and leverage their existing third-party identity provider (IdP) to perform account lockout functions. Customers can also use AWS Directory Service to help comply with this requirement by using fine-grained password policies. The best practice for privileged console access is to restrict traffic to specific workstations, to limit scope, and those workstations be configured to enforce the idle session timeout. “ these are not all of the recommendations that AWS recommends but that i think would be the most important for the company to be compliant to the service.