



Compliance & Security Prioritized:

*A cloud-based approach to PCI
DSS v4 migration*

17th March 2025

CONTENTS

OVERVIEW	03
ADOPTING MODERN SYSTEM COMPONENTS FOR PROTECTING PAYMENT DATA	04
REQUIREMENTS LANDSCAPE	05
BUILDING A PCI-DSS-COMPLIANT ARCHITECTURE ON AWS	08
DELOITTE & AWS - THE ALLIANCE ON THE PCI-DSS IMPLEMENTATION LANDSCAPE	12
CONCLUSION	13
AUTHORS	14



OVERVIEW

In today's highly connected world, securing payment card data is a critical priority for organizations handling sensitive customer information. As cyber threats continue to evolve, the Payment Card Industry Data Security Standard (PCI-DSS) serves as a framework for safeguarding cardholder data across networks and infrastructures. With the release of PCI-DSS Version 4, organizations are now expected to adopt a more flexible, outcome-driven approach to secure cardholder data, enabling them to address complex challenges while maintaining compliance.

This whitepaper provides an overview of PCI-DSS v4 requirements and explores the strategic collaboration between Deloitte and Amazon Web Services (AWS) as it pertains to PCI-DSS framework, emphasizing how the combined services and experience of AWS and Deloitte enables organizations to navigate compliance challenges while enhancing security. It details Deloitte's Cyber framework, which incorporates reference security architecture patterns tailored for AWS environments, and the critical role of PCI-DSS Version 4 in shaping modern cybersecurity strategies.

Through a focus on critical elements such as data classification, network segmentation, identity, and access management (IAM), and automation, this whitepaper demonstrates how Deloitte and AWS are working together to provide scalable, secure, and cost-effective solutions that organizations can leverage to align their cloud environments with the latest PCI-DSS requirements, protect sensitive data and foster innovation and growth in a secure environment.



ADOPTING MODERN SYSTEM COMPONENTS FOR PROTECTING PAYMENT DATA

PCI-DSS serves as a critical framework for securing cardholder data across global networks. The version 4 (v4) of the standard introduces technical and operational baselines, structured into twelve principal requirements and six risk-based security milestones. These advancements to the standard aim to help organizations manage payment account data securely and in an agile manner.

The PCI-DSS Council, established in 2006, by major payment card brands, is an autonomous entity dedicated to improving worldwide security of payment account data. The primary goal of the council is to develop and promote widespread adoption of PCI security standards. The council handles the continual development, enhancement, storage, distribution, and implementation of security standards for the protection of cardholder data.

PCI-DSS v4 expands its scope to include enhanced network security controls, advanced encryption methodologies, refined malware defenses, and broad attack surface management. This version also encourages the adoption of the shared responsibility model, especially in cloud environments, clarifying the roles of cloud providers and organizations, and emphasizing the importance of maintaining data security. Deloitte leverages this shared security model to help organizations navigate the complexities of PCI-DSS and address stringent requirements through a combination of AWS security services and strategic insights.

The adoption of PCI-DSS v4 enables organizations to align with structured security patterns such as data flow, network diagrams, network segmentation, system components and data storage management. These patterns play a crucial role in helping organizations maintain a secure data environment and implementing these patterns within cloud-based frameworks helps organizations adhere to compliance requirements.



REQUIREMENTS LANDSCAPE

PCI-DSS requirements integrate people, processes, and technology into a framework that enhances network controls, account data management, and vulnerability defense. This framework includes organizational policies, monitoring strategies, and structured access controls, collectively safeguarding against security breaches in cloud environments. The framework also outlines the use of compensating controls that help organizations protect systems and comply with PCI-DSS v4 where defined requirements cannot be met due to legitimate technical or business constraints. Enforcing PCI-DSS v4 requirements, helps secure payment systems and align with industry leading practices, in a rapidly evolving digital landscape.

Roles and Responsibilities in the AWS Shared Responsibility Model

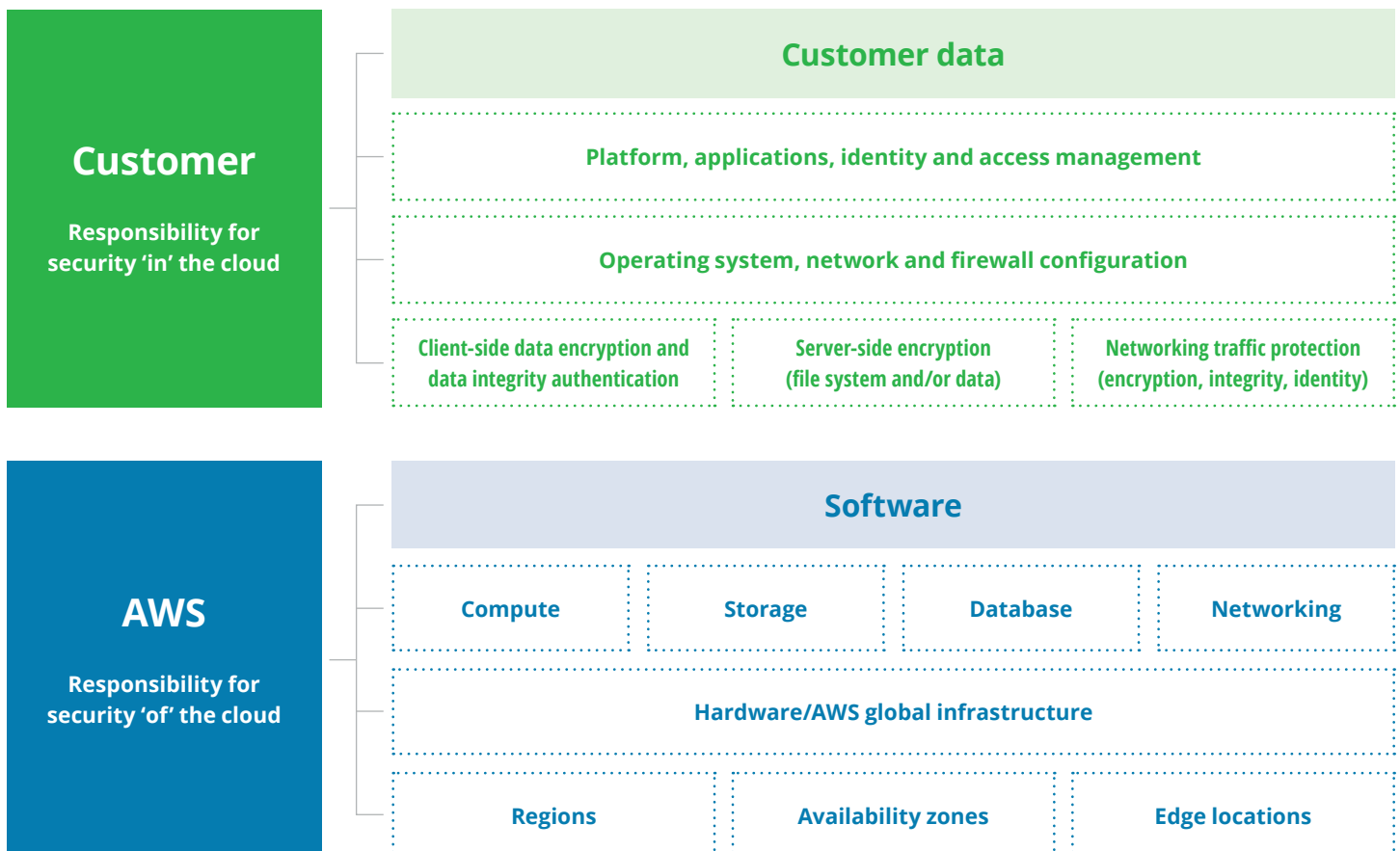
In the realm of cloud security, the AWS Shared Responsibility Model clarifies the division of security roles between AWS and its organizations, complementing the PCI-DSS framework. This model enhances an organization's ability to navigate

through compliance complexities by combining AWS infrastructure security with Deloitte's deep industry experience. Organizations can focus on application security and operational practices within PCI-DSS guidelines, while AWS secures the underlying infrastructure.

AWS is responsible for the security of the cloud infrastructure, including hardware, software, networking, and facilities. This covers the host operating system and virtualization layer. Organizations, meanwhile, can manage their guest operating systems, application software, and security group firewall configurations. Additional considerations for organizations include handling data encryption, secure application protocols, and credential management. This division enables organizations to configure their security practices to meet specific circumstances and requirements, while securely operating in the AWS environment.

AWS services subject to PCI compliance are available in multiple regions, though specific availability can vary. Clients should verify the most current information on service availability by region on the AWS Services in Scope by Compliance Program page to ensure compliance.

Figure 1: Shared Responsibility Model – Customer and AWS



The 6 Risk-based Security Milestones of PCI-DSS in the AWS environment

There are six foundational security milestones of PCI-DSS within the AWS environment, described below. Each milestone focuses on essential security management practices to protect cardholder data and to strengthen network security. The framework lays the foundations for building secure networks, implementing access controls and continuous monitoring. Understanding and working toward these milestones helps organizations enhance data protection strategies, compliance, and add preventative measures against security breaches in AWS-hosted operations.

1) Maintain Secure Network and Systems

In complex cloud environments, it is crucial for organizations to implement a wide range of security measures to monitor data flow across network systems. To protect cardholder data effectively, it is essential to install and maintain a firewall configuration that acts as an enforcement point, guided by organization-specific policies. This firewall controls traffic between various network segments while reducing exposure to untrusted networks, thereby helping reduce the potential attack surface.

In addition to firewall configurations, it is imperative to adhere to leading security practices by avoiding the use of vendor-supplied defaults for system passwords and other security parameters. It is also recommended to apply customized baseline security configurations and timely patches to the underlying infrastructure. These practices are not only vital for resource protection but also help minimizing vulnerabilities and risks.

2) Protect Account Data

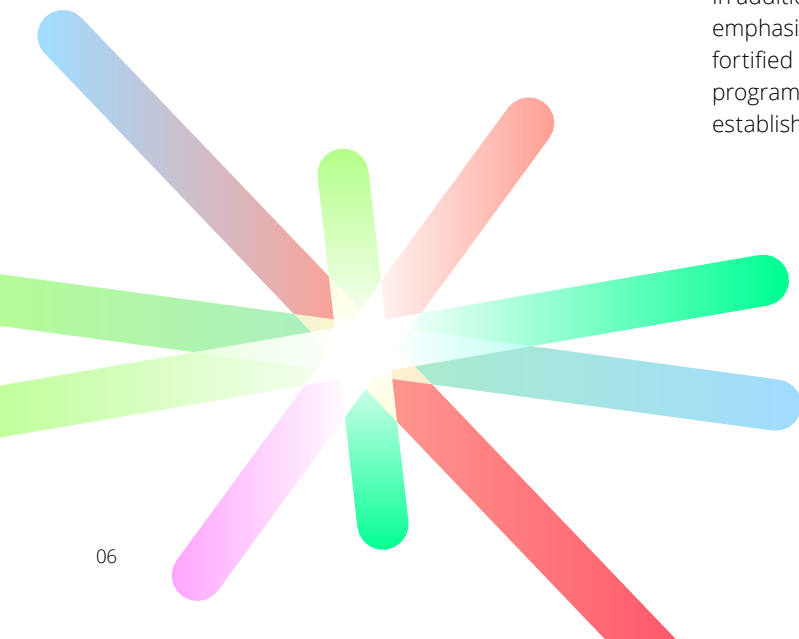
Implementing data protection security controls, such as encryption at rest/in-transit, masking, tokenization, and hashing is crucial to protect the integrity, confidentiality, and availability of data in the cloud. Many of the techniques described above should be considered as potential risk-mitigation opportunities. In addition, the encryption of cardholder data during transmission across open, public networks is highly recommended to augment security while data is in transit.

Automated controls play a critical role in this aspect; capable of scanning, detecting, and remedying potential security misconfigurations. For example, an automated control that helps determine if Sensitive Authentication Data (SAD) is stored post-authentication can significantly aid in addressing compliance with data protection standards.

3) Maintain a Vulnerability Management Program

In the landscape of AWS cloud architecture, it is operationally essential to deploy a multi-faceted Vulnerability Management Program that establishes high level security measures while complying with PCI-DSS standards. This program calls for the integration of automated vulnerability assessment tools into the AWS environment, aimed at continuous identification and timely remediation of system vulnerabilities. It leverages both native AWS security services such as AWS Inspector and third-party insights to develop and maintain secure systems and applications. These tools enable near real-time threat detection and expedite patch management processes, thereby aligning effectively with PCI-DSS requirements for timely security updates and vulnerability management.

In addition to focusing on vulnerabilities, the program emphasizes malware protection. In-scope systems are fortified against malware threats, and antivirus software programs are regularly updated to counter both established and emerging malware threats.



4) Implement Strong Access Control Measurements

In the AWS cloud environment, uncompromising Access Control Measures are not just highly recommended but crucial, particularly when striving for PCI-DSS compliance. This approach extends far beyond basic role-based access controls (RBAC) and involves fully incorporating advanced AWS-native capabilities. These include Identity and Access Management (IAM) policies for identifying and authenticating access to system components, as well as Just-In-Time (JIT) access privileges tailored to the business need-to-know security approach. AWS Cognito is also utilized for federated authentication, further strengthening the identification and authentication process.

To limit and monitor access to cardholder data, dynamic risk-based adjustments are made through AWS IAM Access Analyzer. AWS CloudTrail, which provides a logging mechanism to determine that only authorized personnel have physical or digital access to sensitive cardholder data, can be included to further strengthen access control. Such layers of security provide defense in depth, serving as barriers against unauthorized data and system interactions, thereby upholding the essential principles of data integrity, confidentiality, and availability.

5) Regularly Monitor and Test Networks

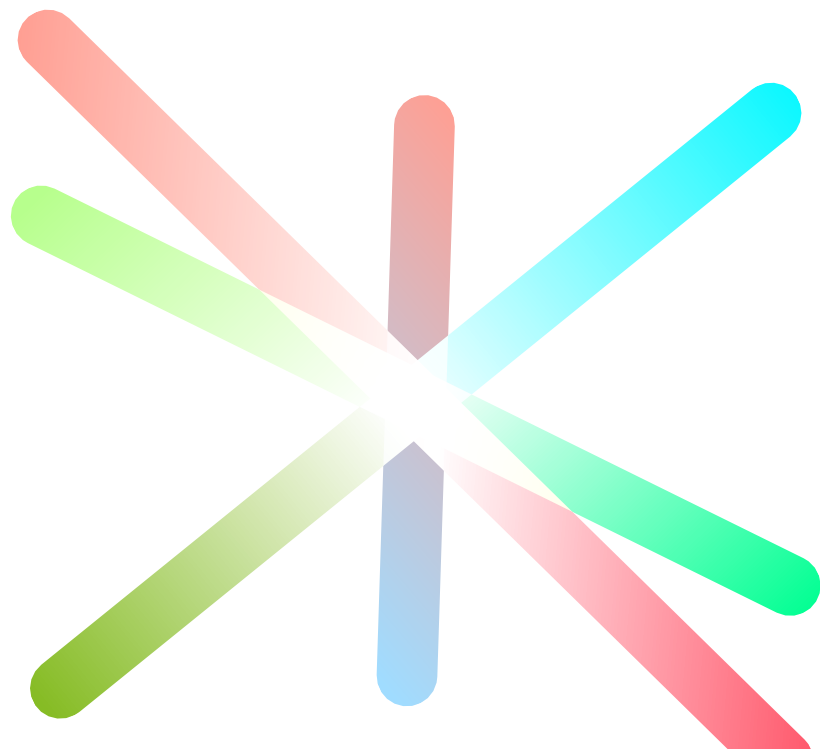
Within the AWS cloud infrastructure, ongoing monitoring and regular security testing are not just recommended practices, but also critical compliance benchmarks set by the PCI-DSS framework. To track and monitor access to network resources and cardholder data, AWS-native services like Amazon GuardDuty are utilized for intrusion detection, while AWS CloudWatch provides real-time log and metric monitoring. This creates an environment that incorporates layered security, while also addressing compliance with data protection requirements.

In addition to continual monitoring, it is imperative to regularly test security systems and processes. This is achieved through alignment with scheduled penetration tests and vulnerability scans, which can be facilitated via tools like AWS Web Application Firewall (WAF) and various third-party integrations. Such rigorous and periodic testing establishes the robustness and effectiveness of the security controls in place.

By embracing this layered approach, which includes near-immediate incident detection and options for automated or semi-automated remediation, organizations can effectively mitigate the risk of potential security breaches. Complying with PCI-DSS requirements that call for continuous monitoring and regular security testing, this approach helps enable a secure, reliable, and compliance-ready operational landscape.

6) Maintain an Information Security Policy

In a perpetually evolving cloud landscape, specifically within the AWS ecosystem, an agile and detailed Information Security Policy serves as the strategic cornerstone for enterprise security governance. This policy should be meticulously crafted to encompass AWS-specific service interactions, data flow models, and potential threat vectors, while being synced with emerging technologies and vulnerabilities.





































BUILDING A PCI-DSS-COMPLIANT ARCHITECTURE ON AWS

AWS provides several solutions and controls to comply with PCI-DSS. However, it is up to organizations to configure their AWS services to meet their own PCI DSS requirements. Organizations can leverage AWS security, identity, compliance, and other services to achieve PCI compliance of their cardholder data environment by configuring required security controls.

There is no one size-fits-all framework that addresses PCI compliance requirements. It is usually a mix and match of frameworks leveraged as leading practices to meet PCI-DSS Compliance. The following [Figure 2] illustrates various AWS services that help you to address the 6 Milestones and 12 Requirements in PCI-DSS requirements.

[Figure 2]: AWS Security Services Ecosystems (not exhaustive) for PCI-DSS Requirements

PCI-DSS Milestones	AWS Services Ecosystem (not exhaustive)					
Build and maintain a secure network and systems	 Amazon VPC	 Container Services	 AWS WAF	 AWS Firewall Manager	 AWS Trusted Advisor	 AWS Systems Manager
Protect cardholder data	 AWS KMS	 AWS CloudHSM	 Amazon Macie	 Amazon S3	 Amazon RDS	 Amazon EBS
Maintain a vulnerability management program	 Amazon Inspector	 Amazon CodeGuru	 Amazon ECR	 AWS Signer	 AWS Network Firewall	 AWS WAF
Implement strong access control measures	 AWS IAM	 Amazon Cognito	 AWS Secrets Manager	 Amazon Verified Permissions	 Amazon Cloud Directory	 AWS Systems Manager
Regularly monitor and test networks	 AWS CloudTrail	 Amazon CloudWatch	 Amazon GuardDuty	 AWS Security Hub	 Amazon Detective	 AWS Config
Maintain an information security policy	 Detective	 AWS Audit Manager	 Amazon GuardDuty	 AWS Security Hub		

The PCI-DSS Security Milestones Implementation using AWS – Overall Approach

Utilizing AWS Config and AWS Security Hub for policy compliance monitoring allows for near real-time adherence checks and triggers automated remedial workflows as necessitated. The result is an updated Information Security Policy that not only satisfies internal governance protocols but also remains in steadfast compliance with PCI-DSS regulations, thus solidifying the organization's overall security stance in a dynamic threat landscape. For example, you can set up PCI DSS-relevant rules on AWS Config to protect cardholder data, especially the select requirements in PCI DSS v4:

- Enabling Multifactor Authentication for IAM users, including root account
- Enabling AWS Key Management Service (KMS) key rotation
- Ensuring system components in the cardholder data environment are not publicly accessible
- Enabling encryption for AWS services like S3, CloudTrail, CloudWatch, DynamoDB, Elastic Kubernetes Service (EKS), Relational Database Service (RDS), Redshift and others as applicable
- Enabling Web Application Firewall on Application Load Balancers and API Gateway by using an AWS WAF Web Access Control List (Web ACL).

1) PCI-DSS Milestone: Build and Maintain Secure Network and Systems

AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. You can protect public facing applications that use Amazon CloudFront distributions, Amazon API Gateway REST APIs, Application Load Balancers, and AWS AppSync GraphQL APIs. AWS WAF can help you meet the following *PCI-DSS requirements v4*:

- **Requirement 1.2.1** - Install and maintain a firewall configuration to protect cardholder data.
- **Requirement 2.2.1** - Develop and maintain procedures to address identified security vulnerabilities.
- **Requirement 6.3.1** - Implement a process to identify and remediate security vulnerabilities in software.

To use AWS WAF for PCI-DSS compliance, you can create a web application firewall and associate it with your web application. You can then use AWS WAF rules to block known vulnerabilities and malicious traffic. AWS WAF also provides a variety of managed rulesets that you can use to protect your web applications from common attacks.



2) PCI-DSS Milestone: Protect Cardholder Data

AWS offers several mechanisms to protect the cardholder data. Amazon S3 offers secure object storage with built-in features such as server-side encryption (SSE) where AWS manages the keys. For additional control, AWS KMS allows the creation and management of the encryption keys, integrating with other AWS services to encrypt stored data. AWS Certificate Manager simplifies the management and deployment of Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates, required for secure data transmission.

3) PCI-DSS Milestone: Maintain a Vulnerability Management Program

"Regularly monitor all audit logs and logs of security events" (Requirement 10 at [Official PCI Security Standards Council Site - Document](#)) is one of specific requirements in PCI-DSS. Amazon GuardDuty is an intelligent threat detection service that continuously monitors your AWS accounts and workloads for malicious activity. Amazon GuardDuty analyzes CloudTrail management event logs, CloudTrail S3 data event logs, Virtual Private Cloud (VPC) Flow Logs, Domain Name Systems (DNS) query logs, and Amazon EKS audit logs. Amazon GuardDuty can also scan Elastic Block Store (EBS) volume data for malware when GuardDuty Malware Protection is enabled and identifies

suspicious behavior indicative of malicious software in EC2 instance or container workloads. The Relational Database Service (RDS) Protection feature adds additional monitoring coverage for suspicious database login events for Amazon Aurora.

Amazon GuardDuty offers advanced detections using machine learning and anomaly detection to identify threats, such as unusual API call patterns or malicious AWS IAM user behavior. Amazon GuardDuty also has integrated threat intelligence, which includes lists of malicious domains or IP addresses from AWS Security and industry-leading third-party security partners.

If potential malicious activity, such as anomalous behavior, credential exfiltration, or command and control infrastructure (C2) communication is detected, Amazon GuardDuty generates detailed security findings that can be used for security visibility and assisting in remediation. Amazon GuardDuty findings are assigned severity, and actions can be automated by integrating with AWS Security Hub, Amazon EventBridge, AWS Lambda, and AWS Step Functions. Amazon Detective is also tightly integrated with Amazon GuardDuty, enabling a deeper forensic and root cause investigation.



4) PCI-DSS Milestone: Implement Strong Access Control Measures

AWS Identity and Access Management (IAM) enables granular control over who can access AWS resources and how the environment has been accessed. Enforcing RBAC through IAM limits access to sensitive data to authorized personnel only, with policies tailored to individual job functions. Multi-Factor authentication (MFA) adds an additional layer of security, and IAM Access Analyzer helps to identify and remediate overly permissive or risky permissions, maintaining the integrity of access controls.

5) PCI-DSS Milestone: Regularly Monitor and Test Networks

AWS provides broad tools for continuous monitoring and testing of network security. Amazon GuardDuty offers intelligent threat detection to monitor for suspicious activity and unauthorized behavior across your AWS environment. AWS CloudTrail tracks user activity and API usage, providing an activity log that can be used for security analysis and operational troubleshooting. Together, these tools enable continuous surveillance and rapid response to potential security issues, aligning with PCI-DSS requirements for regular monitoring and testing.

6) PCI-DSS Milestone: Maintain an Information Security Policy

AWS Artifact delivers on-demand access to AWS compliance documentation, supporting the maintenance of a broad information security policy. AWS Config provides detailed visibility into your AWS resource configuration and changes, intending that security policies are consistently applied and updated as needed. This infrastructure supports the ongoing governance, risk management, and compliance efforts required by PCI-DSS, helping organizations to maintain a secure and compliant cloud environment.

PCI-DSS Recommendation

By leveraging AWS security, identity, and compliance services related to the PCI-DSS requirements, organizations will be able to expedite related business use-cases. Deloitte recommends a standardized approach for enabling PCI DSS v4 controls, given the constraints of the specific changes, compared with previous version (v3.2). The approach begins with methodically assessing the existing cloud environments, identifying gaps, and mapping those gaps to changes related to the PCI DSS v4 model mapping. Deloitte advises organizations to periodically assess their cloud environment so that new findings and remediations will be addressed, considering the latest changes and new challenges addressed upfront by the Deloitte team.

This approach has effectively helped organizations build architecture patterns to remediate the gaps identified by the PCI-DSS v4 model mapping exercise.



DELOITTE & AWS - THE ALLIANCE ON THE PCI-DSS IMPLEMENTATION LANDSCAPE

Strategic Alliances in Cybersecurity:

The Deloitte & AWS Alliance

The alliance between AWS and Deloitte stands as an industry leading alliance in the cybersecurity space. In an era where data security standards, such as PCI-DSS v4 evolve to be more adaptive and outcome-driven, this alliance delivers high-quality insights, embodying leading practices and groundbreaking techniques to safeguard critical data.

Secure By Design: Synergy with AWS

Deloitte's approach does not just protect — it enables businesses. By standardizing access controls and automating security monitoring, Deloitte leverages AWS capabilities to offer a unified network security design that is both adaptable and automated, reflecting the inherent flexibility of PCI DSS v4. The result is a dynamic security architecture that provides businesses with the agility to respond to new threats, maintain operational integrity, and foster innovation.

Deloitte's Cyber framework, strategically utilizing AWS networks and infrastructure and enables the 'Secure by Design' approach, embedding advanced security measures at the core of system development to facilitate business enablement through cyber resilience. This synergy with AWS amplifies the creation of reference security architectures that go beyond precision in design to become enablers of secure business operations, in line with PCI-DSS v4 standards. The transition to a flexible, outcomes-based methodology in PCI-DSS v4 resonates with Deloitte's focus on broad security strategies, fostering adaptability within an array of technological environments. This proactive stance works toward a secure, responsive, and dynamic architecture, ready to confront emerging cyber threats and adapt to technological advancements.

Enhanced Protection: Network and API Security Innovations

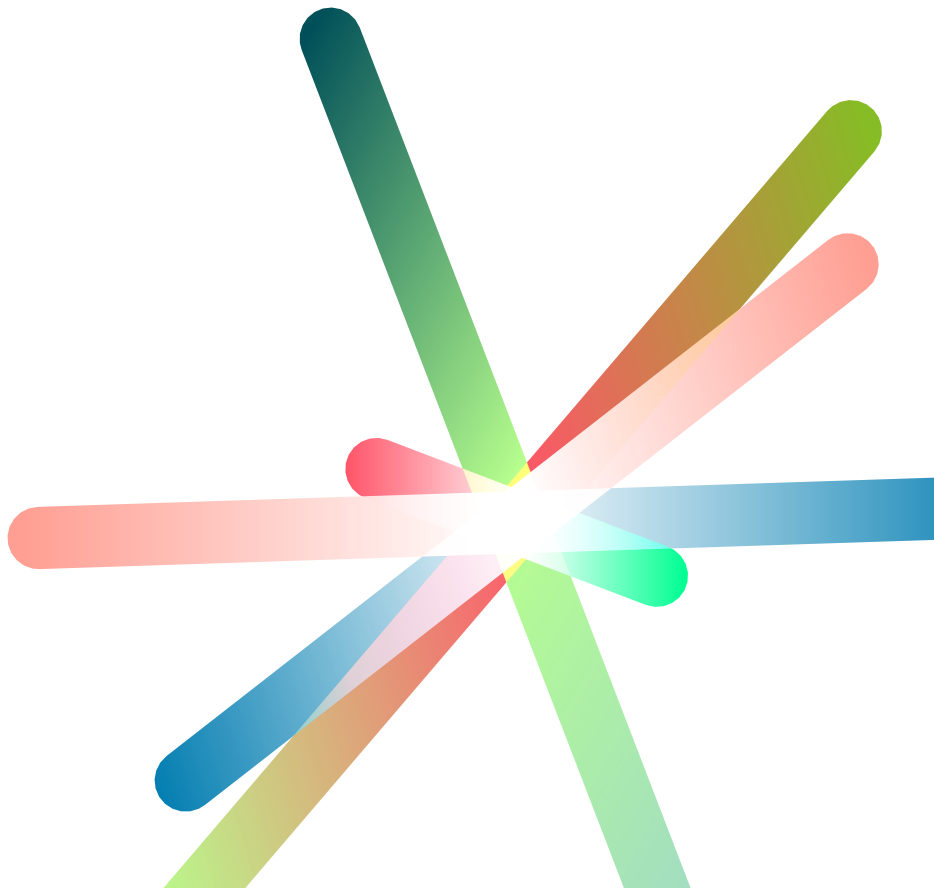
Deloitte and AWS have embraced this paradigm, prioritizing the protection of network traffic, reinforcing endpoints, devices, and safeguarding Application Programming Interfaces (APIs) and services. This collaboration has brought together tools and services to defend entry and exit nodes, establish broad segmentation of internal traffic, implement leading practices in Identity and Access Management (IAM), and provide full visibility into data assets.

Data-Driven Security Architecture:

Beyond Infrastructure

Central to the AWS-Deloitte alliance is the strategic categorization of data within the cloud, whether in processing, transfer, or storage. Considering PCI-DSS v4 prerequisites, design choices are carefully shaped by data categorization. This methodology assists in designing environments using Virtual Private Clouds (VPCs) and subnets, establishing data segregation, effective administration, and automated security configuration. This data-centric approach does not merely configure the environment to specific circumstances but balances risk and cost management, enhancing the objectives of the latest PCI-DSS framework.

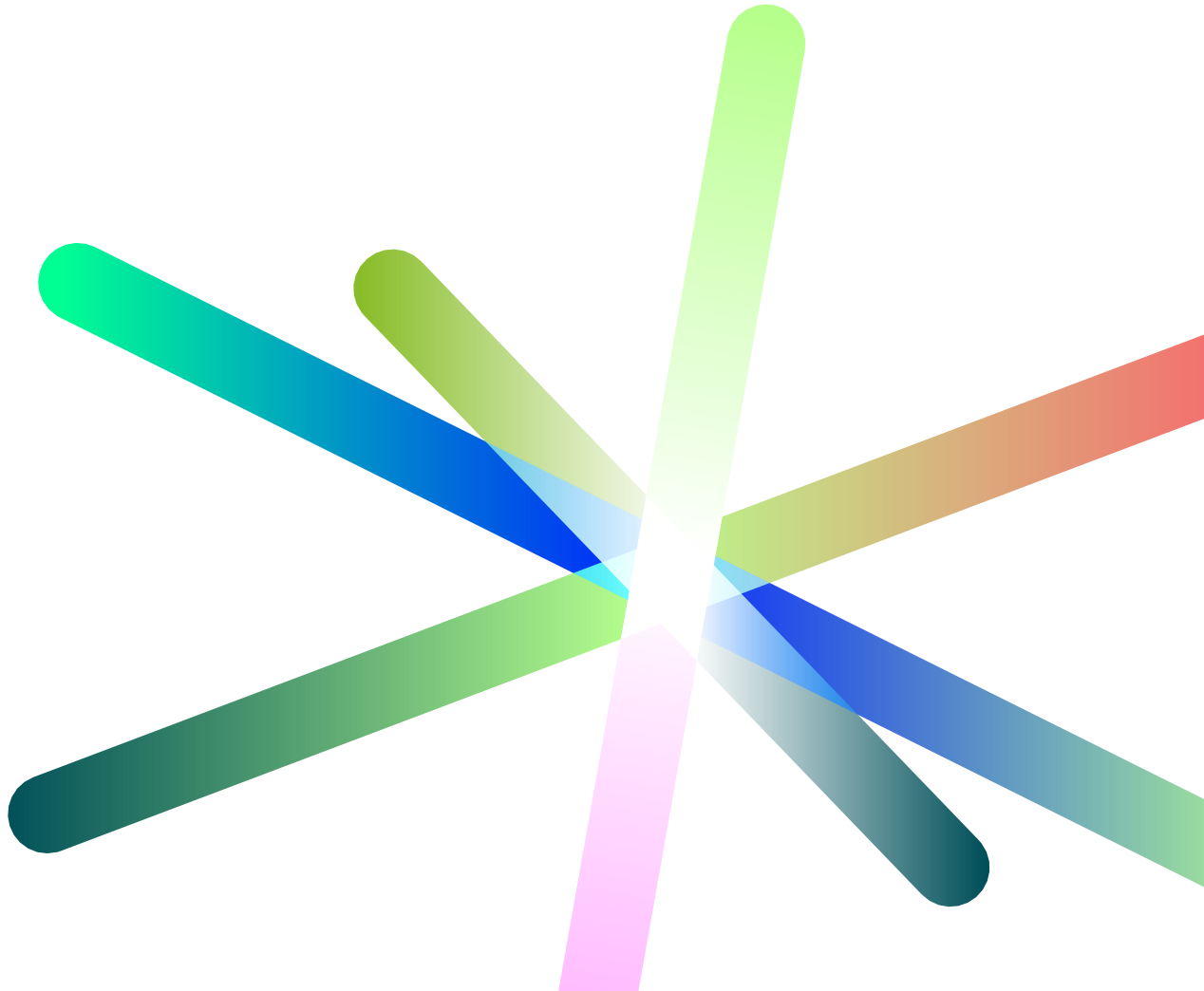
Moreover, the synergy between Deloitte's strategies and AWS's capabilities extends its influence beyond mere network and infrastructure security. Drawing parallels with how a configuration management database (CMDB) addresses threat and vulnerability management, this unified network security design standardizes access controls and security monitoring. The confluence of these components also facilitates effective automation across varied settings, reflecting PCI-DSS's inherent adaptability.



CONCLUSION

When approaching PCI-DSS v4 Cloud Migration, establishing effective security measures for process and technology is crucial to establish a baseline for a strong migration strategy. An effective PCI-DSS implementation strategy should first address gaps with minimal impact, taking into consideration the end- to-end change adoption lifecycle as it moves to addressing higher impact gaps. Additional compensating controls may need to be considered and integrated to strengthen the environment further. By building a strategy around AWS native services and focusing on operational processes related to PCI-DSS framework, organizations can empower teams to adopt security controls upstream of traditional security reviews. The result is that organizations using such a PCI-DSS Cloud Migration security approach make significant strides towards bolstering security and position themselves to embrace the benefits that each framework version has to offer.

For more information on Deloitte's Approach, Security offerings, and to learn how to design an effective PCI-DSS Migration at your organization, reach out to the authors below.



AUTHORS



AARON BROWN

Deloitte & Touche LLP
Partner, Cyber Risk Services
AWS Alliance Leader
Email: aaronbrown@deloitte.com



NIRMAL ARAVA

Deloitte & Touche LLP
Senior Manager,
Cyber Risk Services
Email: narava@deloitte.com



ROBERTO ANDRADE

Deloitte & Touche LLP
Specialist Master,
Cyber Risk Services
Email: roandrade@deloitte.com

SPECIAL THANKS

TAEHYUN (TH) HER

Amazon Web Services
Principal Partner Solutions
Architect, FSI

BARATHI KRISHNAMURTHY

Deloitte & Touche LLP
Manager, Cyber Risk Services
Email: bakrishnamurthy@deloitte.com

LAKSHMI SHANKHWALKER

Deloitte & Touche Assurance and Enterprise
Risk Services India Private Limited
Senior Consultant, Cyber Risk Services
Email: lshankhwalker@deloitte.com

LOUIS DEWITT-HOEGER

Deloitte & Touche LLP
Consultant, Cyber Risk Services
Email: ldewitthoeger@deloitte.com



Deloitte.

This document contains general information only and Deloitte and AWS are not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte and AWS shall not be responsible for any loss sustained by any person who relies on this document.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC.
All rights reserved.

Designed by CoRe Creative Services. RITM2053609