PCI DSS Cloud Compliance Requirements

The Payment Card Industry Data Security Standard (PCI DSS) was created when five credit companies—Visa, MasterCard, American Express, Discover, and JCB—merged their independent security programs into a single industry standard. Today, these companies work collaboratively through the Payment Card Industry Security Standards Council (PCI SSC) to develop and release new versions of the PCI standards.

Who Must Comply with the PCI DSS?
PCI DSS applies to all organizations storing, processing, and handling payment card data, including merchants, acquiring banks, issuing banks, and service providers. The PCI DSS industry group issues the standards, which have a wide range of requirements covering the networking equipment, people, processes, and internal and external applications used to store or process credit card data. The individual payment brands (examples: Visa, American Express) enforce compliance and issue fines for noncompliance. All merchants must adhere to PCI DSS, but smaller merchants (defined separately by each credit card brand) do not have to submit validation of PCI compliance.

What Are the Requirements?
There are 12 main requirements as part of the PCI DSS, and each requirement has detailed sub-requirements. Generally, PCI DSS applies to security controls protecting the primary account number. Whenever an organization stores or handles primary account numbers, they must also secure additional card data, including the cardholder name, address, expiration date, and service code. Organizations may never store sensitive authentication data, including magnetic stripe or chip card data, CVC, CVV, and PIN number.
PCI DSS Requirements

**Build and Maintain a Secure Network**
- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across.

**Maintain a Vulnerability Management Program**
- Use and regularly update antivirus software on all systems commonly affected by malware.
- Develop and maintain secure systems and applications.

**Implement Strong Access Control Measures**
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

**Regularly Monitor and Test Networks**
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

**Maintain an Information Security Policy**
- Maintain a policy that addresses information security.

---

All merchants must adhere to PCI DSS, but only larger merchants must submit annual and quarterly reports. Each credit card brand has different validation requirements. Visa divides merchants into four levels based on their volume and requires validation for merchants that process more than 20,000 Visa transactions per year. Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) perform validation. Annual and quarterly validation steps include:

- Complete Report on Compliance (ROC)
- Perform vulnerability scanning by a PCI SSC-approved scanning vendor (ASV)
- Complete Attestation of Compliance for service providers or merchants, if applicable
- Submit ROC, passing scan, and Attestation of Compliance to acquirer or payment brand

**When Did It Take Effect?**

PCI DSS, Version 3 was released in November 2013. PCI compliance is not required by US law. However, some state laws do refer to PCI DSS, including laws in Minnesota, Nevada, and Washington states.

**What Are the Penalties?**

The payment brand can fine the acquiring bank $5,000 to $100,000 per month, and the bank can pass this fine downstream to the merchant. In practice, this can result in the bank terminating the relationship or increasing transaction fees. A breach can also result in significant legal fees, lost business, and impact to reputation.
How Do You Comply With PCI DSS In The Cloud?
In addition to security measures for on-premise applications, organizations must also consider how their use of cloud impacts their PCI compliance footprint. There are several steps organizations can take to secure card data in the cloud:

- Audit where card data is being stored and transmitted.
- Prevent card data from being uploaded to unsecure cloud applications by enforcing data loss prevention policies across cloud services.
- Many cloud services lack secure password capabilities. Enforce strong password policies using single sign-on solutions.
- Capture audit trails of every user action including user, date and time, result, and affected resource name using a third-party auditing tool if not natively available.
- Regularly audit security using third-party assessors of cloud providers.
- Create an incident response plan and implement an anomaly detection solution across cloud services to detect security breaches.
- Encrypt data stored in cloud services using tenant-managed encryption keys so data is inaccessible to third parties in the event of a breach to reduce liability.