scytale

A PEEK AT PCI DSS

What exactly is PCI DSS Compliance?

Payment Card Industry Data Security Standard (PCI DSS)

Information security standard that ensures all companies who accept, process, store or transmit credit card information maintain a secure environment

Set of 12 security requirements, including the technical and operational standards to best secure and protect credit card data.

Why do you need to be PCI DSS compliant?

✓ **Ensures your infrastructure and business processes are secure when managing customer data.**

✓ **Mandated by the contracts that merchants sign with the card brands and with the banks that handle their payment processing.**

✓ **If you're non-compliant, you can face heavy financial penalties**

Who must undergo a PCI DSS audit?

The audit process differs depending on your merchant-level status:

Category	Criteria	Requirements
Level 1	· Any merchant having more than six million total combined Mastercard and Maestro transactions annually · Any merchant meeting the Level 1 criteria of Vista · Any merchant that Mastercard, in its sole discretion, determnes should meet the Level 1 merchant requirements to miniize risk to the system	Annual PCI DSS assessment resulting in the completion of a Report on Compliance (ROC)1
Level 2	· Any merchant with more than one million but less than or equal to six million total combined Mastercard and Maestro transactions annually · Any merchant meeting the Level 2 criteria of Vista	Annual Self-Assessment Questionaire (SAQ)2
Level 3	· Any merchant with more than 20,000 combined Mastercard e-commerce transactions annually but less than or equal to one million total combined Mastercard and Maestro e-commerce transactions annually · Any merchant meeting the Level 3 criteria of Vista	Annual Self-Assessment Questionaire (SAQ)3
Level 4	· All other merchants	Annual Self-Assessment Questionaire (SAQ)3

How do you get PCI DSS compliant?

Scope:
Determine the components and systems that should be in the scope for PCI DSS and determine your merchant level status.

Assess:
Analyze where your organization's environment is at risk and what areas are not in line with PCI DSS requirements.

Remediation:
Mitigate any vulnerabilities detected to meet PCI DSS standards.

Report:
The assessor and/or entity submits the appropriate documentation according to your merchant-status.

PCI DSS challenges

- Complex and time-consuming process
- Ensuring your organization meets all requirements correctly
- Lack of internal expert-knowledge
- Can't afford risk of non-compliance
- High costs and resources involved, such as consultant costs

How does automation solve the problem?

Automated evidence collection means no manual tasks

Helps organizations get compliant 90% faster

Remain compliant with 24/7 monitoring

Simplified and tailored self-audit

Avoids human error with smart technology

Simplifies control list to meet all PCI DSS requirements

Manages all compliance workflows in one place

Implements policies and procedures with PCI DSS aligned templates

BOOK A DEMO