

# Frictionless PCI Compliance

PCI DSS is the security standard for organizations that store, process or transmit payment card data. If your business accepts card payments, PCI DSS helps prove that cardholder data is being protected through some required controls. Prescient Security delivers practical PCI assessment and testing services, helping organizations evaluate security controls and prepare for successful compliance audits.

## What PCI DSS is

The PCI DSS stands for **Payment Card Industry Data Security Standard** and it is a mandatory security framework for any organization that handles payment card data. It applies to different industries ranging from global enterprises, software companies, merchants, e-commerce providers, and service providers. PCI DSS is more than just a form to complete. Under PCI DSS v4.0 ongoing security is required. Clients need to prove a list of responsibilities like documented controls, evidence of testing, clear ownership and of course the ability to show that your cardholder data environment is properly secured.

Depending on your environment and your bank or payment processor, **customers have two options:**



A shorter Self-Assessment Questionnaire (SAQ)



A more comprehensive Report on Compliance (ROC) and Attestation of Compliance (AOC)

## Why companies need PCI DSS

Companies need PCI DSS because handling payment card data creates real security and business risk. Furthermore, failure to meet those requirements can lead to financial penalties or delays with customers or partners, which should be avoided at all costs.

## So what does PCI DSS include?



**It protects cardholder data:** PCI DSS defines the controls needed to reduce the likelihood of payment data exposure.



**It supports business operations:** Many organizations need PCI validation to sell, transact, or maintain relationships with payment processors and enterprise customers.



**It matters more in cloud environments:** Modern payment systems often span applications, APIs, third parties, and cloud infrastructure, which makes scoping and responsibility mapping especially important.

Many teams are unsure what is actually in scope or which requirements apply to them. This uncertainty often slows PCI efforts down.

# How the PCI process looks with Prescient Security

Prescient Security takes a practical, QSA-led approach that helps clients define scope correctly and move through the assessment with a clear plan. Let's take a look at the process step by step:



## Scope the environment

We start by understanding how your organization handles cardholder data and what your acquiring bank or payment processor expects you to submit. That includes whether you store, process, or transmit cardholder data, what cloud platforms you use, and whether you may qualify for an SAQ or need a full ROC.

We also look for **opportunities to reduce scope**. For example, if you use a data vault provider, some responsibility can be shifted outside your environment, which may reduce both risk and assessment complexity.



## Review evidence and perform the assessment

Once scope is defined, Prescient Security assigns a QSA and kicks off the engagement. If you use a GRC platform we can work from the evidence already organized there. If not, we support manual evidence collection through a structured gap analysis and shared documentation process.

**Our team reviews submitted evidence first, then uses interviews to close only the gaps that could not be confirmed through documentation.** This keeps the process focused and reduces unnecessary meeting time for your internal teams.



## Deliver the compliance report

After evidence review and interviews, we **prepare a draft report for client review, complete internal peer quality assurance, and finalize the deliverable**. For larger Level 1 assessments, this typically results in a ROC and AOC. For smaller, lower-scope environments, SAQ assessments can move much faster.

What makes Prescient Security different: **Clients work with one partner across scoping, assessment, testing coordination, and final compliance reporting.** That means less vendor coordination, clearer ownership, and a more streamlined path to completion.

## Why organizations choose Prescient Security

- 1 QSA-led guidance that helps clients determine the right path, from SAQs to full ROC assessments
- 2 Flexible evidence collection through existing GRC systems or manual workflows
- 3 Security-first scoping that helps reduce the cardholder data environment where possible
- 4 End-to-end support from readiness through final compliance deliverables

From scoping and readiness to certification, Prescient Security helps organizations secure cardholder data and navigate PCI DSS requirements with confidence.