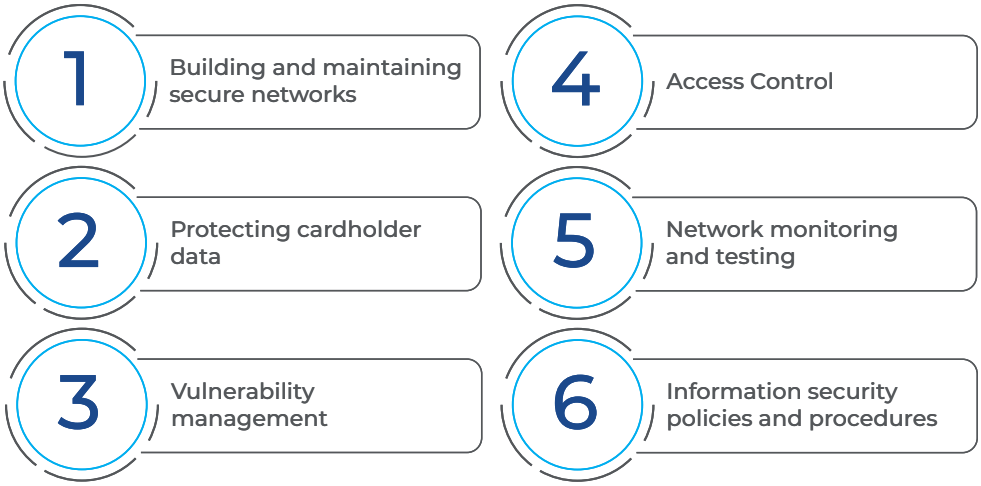
CompliancePoint®

Getting Started with the PCI DSS

What is the PCI DSS?

The PCI Security Standards Council (SSC) was started in 2006 by American Express, Discover, JCB, Mastercard and Visa with the goal of minimizing fraud and improving transaction security for the payment card industry. The SSC defines, implements, and maintains the Payment Card Industry Data Security Standard (PCI DSS).

The standard includes six main areas of focus:



The PCI DSS applies to all organizations involved in the processing of payment card information. This includes merchants, processors, acquirers, card issuers and other service providers. Anyone involved in the storage, processing or transmission of PCI Account Data is in-scope for the PCI DSS.

All PCI "Account Data" falls under the requirements for the PCI DSS. Account data can be broken out into two main areas:

Cardholder Data	Sensitive Authentication Data (SAD)
Primary Account Number (PAN)	Full Track Data
Cardholder Name	CVV/CAV/CVC/CID
Expiration Date	PIN/PIN Blocks
Service Code	

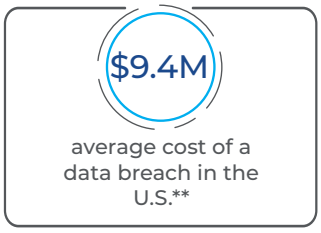
PRO TIP: Most online organizations do not process SAD.

Why is it Important?

The PCI DSS is important because it helps to enable trust between consumers and the businesses involved in handling their Payment Card information. The consequences of a breach of this information can damage your brand and customer reputation, resulting in a material impact to your organization's sales and value. Most organizations are contractually bound to meet the requirements of the PCI DSS. This is accomplished within merchant agreements on the consumer side or through business contracts with service providers. The good news is that a PCI DSS certification helps to create trust with the consumer, can provide safe harbor, and may reduce fines and the costs from a data breach.

What Does it Mean to Be Compliant?

Demonstrating compliance with the PCI DSS generally means that you have the appropriate security controls implemented to protect your customers' Account Data. Tracking your compliance is best broken out into three main areas: 1) Governance, 2) Operations and 3) Technology. PCI DSS is complicated, with over 350 potential control requirements that could apply. The applicable controls for your environment are beyond the scope of this document. We recommend you reach out to us at connect@compliancepoint.com to consult with one of our PCI DSS Qualified Security Assessors (QSA) to better understand how this standard applies to your specific environment.



What Are the Reporting Requirements?

Merchant		Self-Assessment Questionnaire (SAQ)	Report on Compliance (ROC)
LEVEL 1	Over 6 million transactions		✓
LEVEL 2	1 to 6 million transactions	✓	
LEVEL 3	20,000 to 1 million transactions	✓	
LEVEL 4	Fewer than 20,000 transactions	✓	

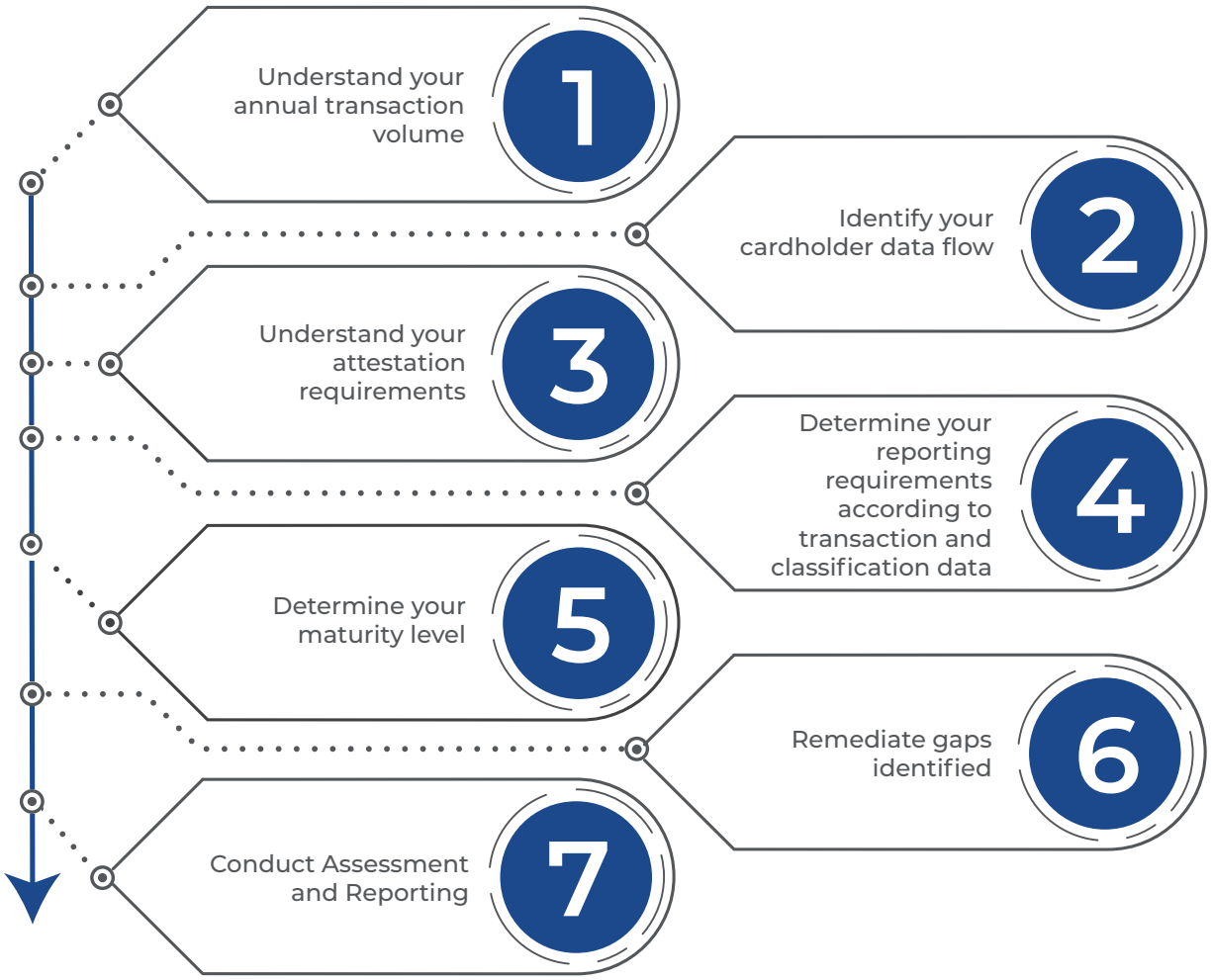
Service Provider		Self-Assessment Questionnaire (SAQ)	Report on Compliance (ROC)
LEVEL 1	More than 300,000 transactions		✓
LEVEL 2	Fewer than 300,000 transactions	✓	

In the event of a breach, some merchants or service providers may require enhanced reporting.

PRO TIP: Understand if you need to be compliant or certified, and understand the difference.

* Atlas VPN research (https://atlasvpn.com/blog/47-percent-americans-find-identity-theft-worse-than-murder-new-report-show)
** IBM – Cost of a Data Breach 2022 (https://www.ibm.com/reports/data-breach)

What Does the Certification Process Look Like?



PRO TIP: Most organizations are about 25% compliant when starting out.

Maturity Checklist

For organizations looking to demonstrate compliance with the PCI DSS, it is imperative that they conduct a readiness assessment. This effort will help project stakeholders better understand organizational maturity and assess the effort required to demonstrate compliance with the standard. A readiness assessment is one of the primary services CompliancePoint provides to clients who are getting started in the process of certification.

PRO TIP: Don't store cardholder data if you don't have to.

The checklist below can be used as a starting point to measure the organizational maturity relative to the PCI DSS. In general, organizations should expect to score a 3 or better before attempting certification.

Governance Requirements	1-Initial	2-Managed	3-Defined	4-Quant.	5-Optimized
Acceptable use policy					
Risk Assessment Policy					
Vendor Management Policy					
Software Development					
Incident Response					
Information Security Policy					

Operational Requirements	1-Initial	2-Managed	3-Defined	4-Quant.	5-Optimized
Security Awareness Training					
Employee Background Checks					
Physical Access Controls					
Visitor Handling Procedures					
Media Handling and Backup Procedures					
Change Control Procedures					
Hardening Guidelines and Configuration Standards					
Vulnerability Management Process					
Security and Event Monitoring Procedures					

Technical Requirements	1-Initial	2-Managed	3-Defined	4-Quant.	5-Optimized
IDS/IPS System					
Access Control System (Logical)					
Anti-Virus System					
Network Diagrams					
Documented Cardholder Data Flow					
Encryption of Cardholder Data					
Wireless Security Controls					
Web Application Firewall					

The actual control requirements and their applicability are far more nuanced than the checklist above. CompliancePoint recommends that you engage a QSA early in the process to gain the best understanding of how the PCI DSS requirements apply to your specific environment.

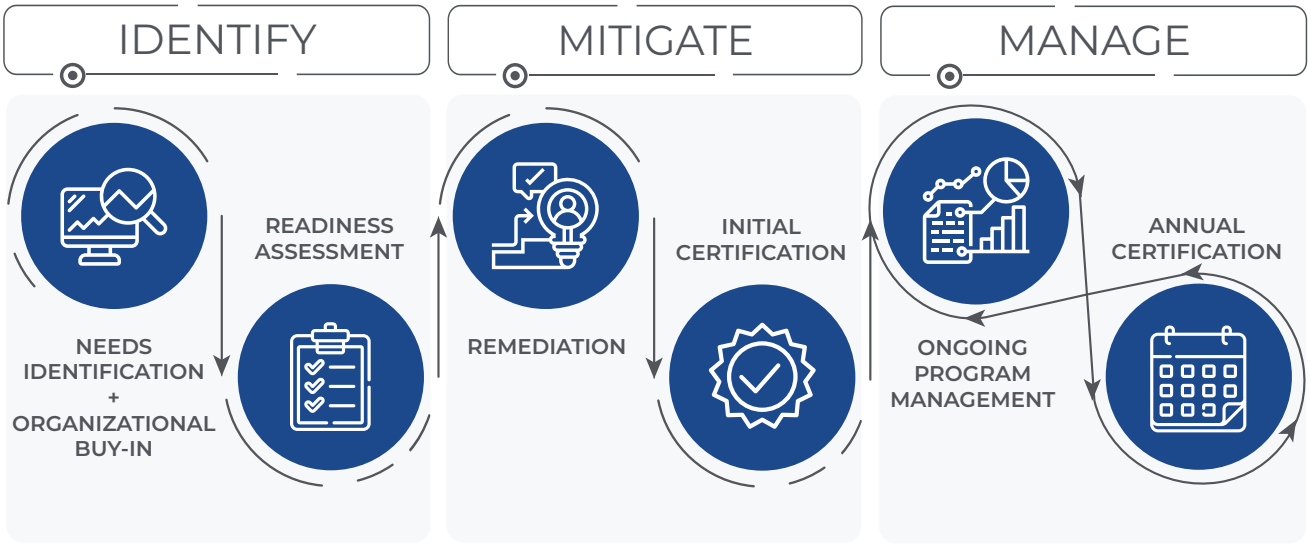
Got questions about your environment?
Click here to speak with a QSA!

NEED HELP?

PRO TIP: Design your cardholder data environment to be as small as possible.

How CompliancePoint Can Help

CompliancePoint provides a full suite of services that help organizations manage and respond effectively to compliance requirements. Using our IDENTIFY, MITIGATE + MANAGE approach, we help organizations proactively identify their gaps, build out frameworks to meet compliance requirements and help manage long term programs to maintain this posture.



ASSURANCE SERVICES

IDENTIFY	MITIGATE	MANAGE
• Readiness/Gap Assessments • Risk Assessments • Roles & Responsibilities Mapping (Service Providers) • Vulnerability Scanning & Penetration Testing • CDE Design & Strategic Consulting	• ASV Scanning • Managed Security Services • Remediation Consulting • Policy & Procedure Development • SAQ Assistance • Security Awareness Training • Security Control Design and Implementation	• Compliance and Security Program Management • Ongoing Risk Management • Ongoing Annual Certification(s) • Vulnerability Management

About CompliancePoint

CompliancePoint is a leading provider of risk management services focused on information security, data privacy, and compliance. Organizations face many risks associated with engaging their marketplace including how they process information internally and with whom they share information downstream. Our mission is to help our clients interact responsibly with their customers and the marketplace.

The difference is simple – data privacy, security and compliance have been at the core of our service offering for almost two decades. We provide our clients with a broad view of industry best practices and benchmarking that allows our customers to make informed business decisions, helping to minimize impact to business operations and maximize return on investment.

- Business-centric approach
- Full lifecycle support
- Company-specific recommendations
- Over 2,500 companies assessed
- True practitioners with hands-on experience
- One of the original 20 assessment companies for PCI