

# Beginner's Guide to PCI Compliance

PCI DSS audits are intimidating. This guide will make sure you know what you need to successfully complete a PCI audit.



# PCI audits are hard.

We believe if you're going to do an audit, it should be worth it.

We know that when it comes to threats you want to make sure you're ready. In order to do that, you need a quality PCI audit report that gives you results you can trust and that gets you on the VISA compliance list. The problem is PCI audits are hard, and the complicated process feels overwhelming.

This guide should help make your PCI audit a little less complicated and a little easier to get started.



## Table of Contents

|    |   |
|----|---|
| 3  | An Intro to PCI                             |
| 4  | How a PCI Audit Benefits Your Organization  |
| 5  | What You Need to Know Before Your PCI Audit |
| 6  | How the PCI Audit Process Works             |
| 8  | The 12 PCI Requirements                     |
| 9  | PCI Policy Requirements                     |
| 12 | Starting Your Audit                         |

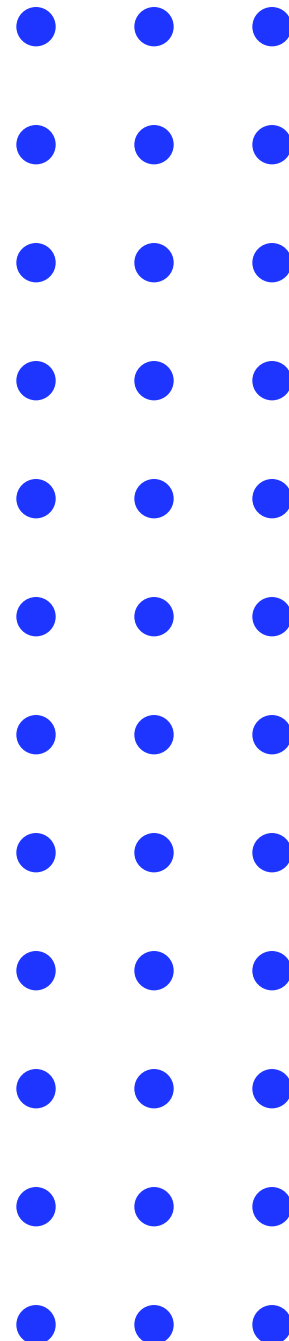
# An Introduction to PCI DSS

In December 2004, major credit card companies, including Visa, MasterCard, American Express, Discover, and JCB, acted against the increased number of data security breaches by coming together to create the PCI Security Standards Council. This Council developed a security standard for merchants that process credit card data, known as the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS encourages and enhances cardholder data security by providing globally recognized data security measures.

Merchants, service providers, and subservice providers that store, transmit, or process cardholder data, including credit, debit, or other payment cards, are required to adhere to the Payment Card Industry Data Security Standard (PCI DSS).

The PCI audit is designed to test whether your organization is compliant with the 12 technical and operational requirements established to protect cardholder data. These 12 requirements are outlined later in this guide.

A successful PCI audit engagement culminates in your organization being included on the [Visa Global Registry of Service Providers](#). This list is the industry standard that allows service providers to show off their compliance with the PCI DSS standard.



# How a PCI Audit Benefits You

As a client or vendor, you want your organization to be seen as preventive and protective, but compliance is not an option when it comes to cardholder data. PCI DSS ensures that an organization can help prevent losses and protect cardholder data. Many organizations will only work with PCI compliant businesses, which opens up opportunities for you to gain more clientele. Alternatively, you could lose clients if non-compliance causes your organization's reputation to decline.

If you are found to be non-compliant with PCI DSS you could face a number of consequences, the costliest being severe fines ranging from \$5,000 to \$500,000. This amount does not consider any additional costs from reissuing cards to victimized cardholders, credit monitoring, remediation and investigation actions, and increased rates charged by banks or processors. Credit card companies could even revoke your right to process credit card transactions depending on the severity of any actions resulting from PCI non-compliance.

Don't leave your reputation, clients, or card payment processing abilities up to chance. Pursue a PCI audit so that your organization is compliant with PCI DSS, and so you can have peace of mind about your business practices and cardholder data.

# What You Need To Know Before Your PCI Audit

When it comes to preparing for your PCI audit and securing your cardholder data environment (CDE), it's important to understand where all of your sensitive assets lie. Taking an inventory to identify any and all locations with stored cardholder data and performing a thorough search of all systems to identify cardholders and track data is a critical PCI audit preparation step.

The scope of your CDE determines the extent to which all PCI DSS controls must be in place. Common issues with PCI compliance are a result of scoping errors. Any personnel, processes, or technologies that store, process, or transmit cardholder data, are considered to be within your CDE and therefore in scope for your PCI audit. These assets include:



Any devices that provide security/authentication services, such as firewall, router, or patching server



Any asset that is connected to the CDE



Any routing rules that allow traffic into the CDE



Any asset that can impact CDE security in any way

To reduce the scope of your PCI audit and assessment, you can use logical and physical controls to ensure network segmentation. Segmentation is the use and implementation of additional security controls to separate systems with different security needs. These controls commonly include firewall and router configurations to deny traffic passing from out-of-scope networks and the CDE, network hardening standards, and physical access controls.

# How the PCI Audit Process Works

A PCI audit is a rigorous examination of the Payment Card Industry Data Security Standard, which consists of nearly 400 individual controls and is a critical part of staying in business for any merchant, service provider, or subservice provider who is involved in handling cardholder data.

At KirkpatrickPrice, our PCI audit program takes a seven-step approach to help your organization gain PCI compliance.

## 1 Gap Analysis

Before you begin a PCI audit for the first time, we recommend going through a gap analysis.

A gap analysis helps to identify any administrative, physical, and technical gaps in your information security program; specifically, in the way that you handle cardholder data. Going through a gap analysis allows our senior-level QSAs to understand your business and your level of readiness for a PCI audit. The gap analysis is an important step towards PCI compliance because your QSA can create remediation strategies that will guide you through the PCI audit process and towards compliance. Next, your organization will move on to remediate the findings found during the gap analysis.

## 2 Remediation

Now that your organization understands its administrative, physical, and technical gaps, a QSA from KirkpatrickPrice will work to develop a detailed remediation plan with findings from the gap analysis and recommendations on proper ways to mitigate areas of non-compliance. The remediation step in the PCI audit process will help your organization to recognize its gaps and remediate those areas for a smoother path towards PCI compliance.

## 3 Scoping and Planning

Next, it's time to start the PCI audit by verifying the scope of the engagement. We will work with your organization to analyze your services, geographic locations, payment applications, third parties, and other system factors to develop an accurate scope for the PCI audit. The narrower the scope, the more accurate and efficient your PCI audit process will be, so we aim for a detailed and defined scope. The scoping and planning stage prepares the entire engagement team to move to the next step of gathering information.

## 4 Gathering

At KirkpatrickPrice, we will collect your policies, procedures, and other documentation needed for your PCI audit through the Online Audit Manager. Alongside your designated QSA, you will begin answering questions and describing systems relating to your organization's internal controls. This allows the audit team to accurately assess the full scope of your audit for the PCI engagement. Your QSA will test and evaluate the operational effectiveness of those controls according to the prescribed PCI requirements.

## 5 Onsite Visit

Onsite visits during the PCI audit process are important for not only testing internal controls that cannot be accurately tested remotely, but also seeing your people and technology in-action. During the onsite visit, a senior-level QSA, who has been partnered with you throughout the PCI audit process, will observe and test your organization to determine if your processes meet the 12 requirements of PCI compliance.

## 6 Report Delivery

The sixth step in the PCI audit process is receiving a Report on Compliance (RoC), which provides you with a detailed report on the results from your PCI audit. To generate RoCs, KirkpatrickPrice has a team of Professional Writers, who are trained and knowledgeable about the PCI DSS, that write high quality reports. Your report will also go through our Quality Assurance processes to ensure it meets our quality standards. You can take a deep breath knowing your PCI audit was performed by a QSA and a firm that is committed to your organization's compliance success!

## 7 Get on the List

We know the ultimate goal of completing a PCI audit is getting on the Visa Compliance List to give your clients an added level of assurance. By completing all the steps of your PCI DSS audit with a qualified auditing firm, you'll receive a report that will help you get on the list.

# The 12 PCI Requirements

The 12 PCI DSS Requirements were designed to decrease credit card fraud by increasing the controls involved in protecting cardholder data. This is a framework for merchants, service providers, and sub-service providers to develop a strong payment card data security process, including prevention, detection, and reaction to security incidents. The RoC issued to your organization will include findings as they relate to the following 12 PCI DSS Requirements:

## **Build and Maintain a Secure Network**

- **Requirement 1:** Install and maintain network security controls to protect cardholder data.
- **Requirement 2:** Apply secure configurations to all system components; do not use vendor-supplied defaults for system passwords and other security parameters.

## **Protect Cardholder Data**

- **Requirement 3:** Protect stored cardholder and account data.
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.

## **Maintain a Vulnerability Management Program**

- **Requirement 5:** Protect all systems and networks from malicious software by using and regularly updating anti-virus software.
- **Requirement 6:** Develop and maintain secure systems and software.

## **Implement Strong Access Control Measures**

- **Requirement 7:** Restrict access to cardholder data by business need-to-know.
- **Requirement 8:** Log and monitor all system access by assigning a unique ID to each person with computer access.
- **Requirement 9:** Restrict physical access to cardholder data.

## **Regularly Monitor and Test Networks**

- **Requirement 10:** Log and monitor all access to network resources and cardholder data.
- **Requirement 11:** Regularly test security systems, network, and processes.

## **Maintain an Information Security Policy**

- **Requirement 12:** Support your information security efforts with policies and programs.



# PCI Policy Requirements

---

Each of the 12 requirements includes a specific sub-requirement to ensure that security policies and operational procedures are documented, in use, and known to all affected parties. Why? Because knowing and using policies and procedures is a way of managing your organization's assets and environment; it is not sufficient to generate the documentation just for the sake of a PCI audit, then never use or implement the policies and procedures.

Many organizations struggle with the documentation aspect of a PCI assessment. Established best practice states, "If it's not written down, it's not happening." Organizations need documented policies, procedures, and standards to control risks to business assets, but to also have a common understanding and language that creates consistency amongst your organization.

# Policies that Align with PCI Requirements

Depending on your unique services, industry, legal requirements, or other frameworks outside of PCI that you must comply with, there will be various topics that your information security policies should cover. PCI DSS does a good job of outlining which policies you absolutely need to begin a baseline set of PCI-compliant policies.

A recommended set of information security policies and procedures that align with PCI requirements should include the following topics:

## Requirement 1

- Firewall Configuration Standards and Operational Procedures
- Operational Procedures for Managing Firewalls

## Requirement 2

- Operational Procedures for Managing Vendor Defaults and Other Security Parameters

## Requirement 3

- Data Retention and Disposal Policies
- CHD Storage and Protection Policies

## Requirement 4

- Encryption Key Management Policies and Operational Procedures
- Operational Procedures for Encrypting Transmissions of CHD

## Requirement 5

- Anti-Virus and Malware Software Policies
- Security Patch Installation Policies

## Requirement 6

- Software Development Policies and Operational Procedures
- Change Control Policies and Operational Procedures

**Requirement 7**

- Access Control Policies and Operational Procedures

**Requirement 8**

- User Identification Management
- Authentication Policies and Procedures

**Requirement 9**

- Procedures for Onsite Personnel and Visitors
- Physical Security Policies

**Requirement 10**

- Audit Log Retention Policies
- Security Control Failure Response Policies
- Policies for Access to Network Resources and CHD
- Policies for Detection and Identification of Wireless Access Points
- Procedures for Detection of PAN Outside the CDE

**Requirement 11**

- Penetration Testing Procedures
- Security Monitoring and Testing Procedures
- Procedures to Review Hardware and Software Technologies

**Requirement 12**

- Information Security Policy

**Please note:** This list serves as an overview of what policies and procedures should be documented and implemented when pursuing PCI compliance, but it is not an all-encompassing list. For more information on the specific details of what needs to be included in each policy or procedure, we encourage you to review the current PCI DSS framework or contact your QSA.



# Partner with KirkpatrickPrice to Meet All of Your Compliance Goals

Going through a PCI engagement can be confusing and rigorous, but when you partner with KirkpatrickPrice, it doesn't have to be. We've been in your shoes and know how challenging it can be to get on the Visa compliance list. You'll partner with senior-level experts and QSAs with years of PCI experience across many disciplines.

When you work with KirkpatrickPrice, you can stop feeling like you are going to miss something or be surprised when a client or attacker finds something that wasn't in your report. You can stop feeling worried that you're wasting time using someone who isn't advanced enough to thoroughly test your environment. Instead, you'll have a report that gets you ready for your next steps, allows you to say yes to client requests, and brings you the assurance you deserve. Cybersecurity and compliance will no longer be a mystery.

To get started on your PCI audit, call one of our experts today at 800-779-2701 or visit [www.kirkpatrickprice.com](http://www.kirkpatrickprice.com).

---

P.S. – Let's stay connected! Follow KirkpatrickPrice on LinkedIn, subscribe to our YouTube channel, or sign up for our monthly newsletter, The Readiness Report.

