RECIPROCITY

Preparing for a PCI DSS Audit

Five Steps to Success

www.reciprocitylabs.com

If your organization accepts payment cards, it must comply with the Payment Card Industry Data Security Standard (PCI DSS): twelve objectives that spell out a long list of requirements. PCI DSS was established in 2006 by the PCI Security Standards Council, which comprises financial institutions, merchants, processor companies, software developers, and point-of-sale vendors.

Established to protect consumers, banks, and credit card vendors from data theft and fraud, PCI DSS is not a regulatory framework, but rather an industry one. Nevertheless, the price of noncompliance can be steep: hefty fines each month until compliance is reached, or—possibly worse—the loss of credit card transaction privileges.

In this day and age, having to say, "Sorry, we don't accept credit cards" can be a death knell for any enterprise.

Audit or Self-Assessment?

Not every merchant needs a full-blown external audit to satisfy the PCI Security Standards Council. Only those with a large number of annual payment card transactions—1 to 6 million or more for merchant levels 1 and 2 on some major cards—will need to show a Report on Compliance by a Qualified Security Assessor or Internal Security Assessor. Merchants processing fewer payments can self-assess.

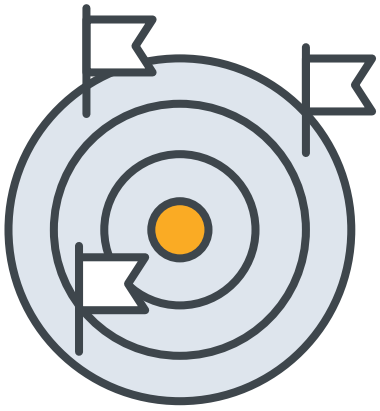
Anyone new to a PCI DSS audit may feel daunted by the plethora of requirements and directives. Admittedly, achieving compliance is no easy task, and maintaining it can be challenging, too. As the threat landscape changes and technology evolves, so do the PCI standards. To date, revisions have been issued every few years—some minor, others with many changes.

However, PCI DSS is written to make compliance achievable, no matter the organization's merchant level or expertise. Do your work in advance by following these steps, and you should have no trouble passing a PCI DSS audit and keeping your enterprise's payment card transactions—and the business—running smoothly.

1 Determine your scope.

Sit down with the PCI DSS requirements—all 281 of them—and scrutinize each and every one, identifying those with which your organization needs to comply.

Not all requirements apply to every merchant, so identifying the appropriate scope will reduce your work and increase the auditor's efficiency.



The standard stipulates the precise steps you must take to protect payment card transactions in your cardholder data environment (CDE), which includes:

- Point-of-sale devices
- Mobile devices, personal computers, and servers
- Wireless hotspots
- Internet shopping applications
- Paper-based storage systems
- The transmission of cardholder data to service providers
- Remote-access connections

If this is your first experience with a security framework, you may find the long list of requirements intimidating at first. After spending some time with the document, however, you will find that, unlike other regulatory frameworks, PCI DSS is fairly user-friendly. It's prescriptive, telling you exactly what you must do to comply, and it's specific, aimed at protecting one type of information: payment card data. Security and compliance professionals should find the document comprehensible and clear. If not, you may need the help of a PCI-savvy consultant or auditor, or quality compliance software.

A caveat: although PCI spells out steps and suggestions for fulfilling its objectives, meeting them all is time-consuming and often requires a complex series of tasks, especially for larger organizations.

Give your enterprise ample time to prepare, especially for that first audit. Your scope-defining list will help you determine how long you will need to get ready.

2 Minimize your scope.

There are things you can do pre-audit to minimize the risk to your payment card data and devices and, therefore, to narrow the scope of your PCI DSS audit, potentially saving time and expense.

Limit access to your CDE with firewalls.

Requirement 1.2.1 of PCI DSS advises, "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic."

To do this, the framework requires an entity to "install a network firewall between the CDE and corporate network to ensure only designated systems in the corporate network can communicate, via approved ports, to systems in the CDE. Additionally, the entity may use the same, or another, firewall to block all connections and prevent access between the CDE and an out-of-scope network. In this way, a firewall is being used to implement a PCI DSS requirement for in-scope systems and network, and is also used to segment an out-of-scope network."

Firewalls are one way to block access, keeping external users from entering your networks as well as keeping internal users from gaining access to information they do not need.

Encrypt everything.

Do you use point-to-point encryption from the moment a cardholder submits their information all the way through payment processing? Encryption likely will minimize the scope and cost of your audit. Make sure you're using point-of-sale devices, software, and point-to-point encryption devices that have been approved by the PCI council.

Analyze your third-party vendor functions.

If your enterprise outsources any functions in the scope of PCI DSS or uses a third-party service that could affect PCI DSS compliance, make sure the vendor or function complies with the framework's requirements. It is also important to establish a clear delineation of responsibilities for each requirement.

Analyze your third-party connections.

Requirement 2.1 states, "In addition to including internal systems and networks in scope, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls must then be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE."

If your organization is small and uses a third-party application to handle all its payment processing, you need to make sure that processor is PCI DSS compliant. If you retain any payment information, you may opt to use a PCI-approved payment application, recommended (but not required) by the PCI Security Council. If you want to use a payment application that isn't already certified, you will need to obtain PCI approval for it—a process that can require much time and effort. Either way, you will be responsible for ensuring that the application retains its PCI Security Council approval and for staying current with patches and updates.

Segment your networks.

PCI DSS recommends but does not require isolating the CDE from the rest of your enterprise's network.

It states: "Network segmentation of or isolating (segmenting) the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- *The scope of the PCI DSS assessment*
- *The cost of the PCI DSS assessment*
- *The cost and difficulty of implementing and maintaining PCI DSS controls*
- *The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations"*

Without adequate network segmentation (a "flat network"), your entire network will be in scope for a PCI DSS audit.

If you place firewalls around your CDE network, however, the audit will apply only to the portion of your environment where payment information is collected, processed, and stored.

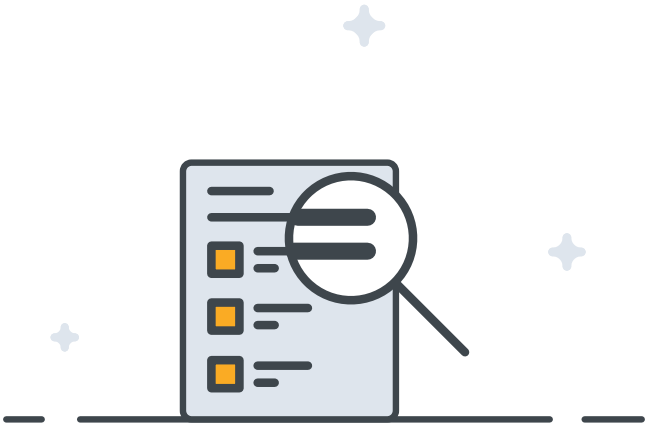
Segmentation begins with an examination of the people, processes, and technologies that interact with cardholder data.

- Identify all payment channels and methods for accepting, processing, and storing cardholder information, from the point of receipt to the point of destruction, disposal, or transfer. Include all systems within and connected to the CDE.
- Implement controls that restrict access to this segment to those who need it.
- Make sure that in-scope and out-of-scope networks do not communicate.
- Avoid transmitting cardholder data using wifi, if possible.

Dispose of cardholder data promptly and effectively.

Keep only the information your enterprise needs, for only as long as necessary. When destroying data, use one of the PCI Security Council's approved methods.

3 Determine how well you meet each applicable requirement.



Examine each item on your list to determine how well you comply with each applicable objective and sub-objective.

The PCI website offers tools, including self-assessment questionnaires, to help with this step.

4 Test your controls.

Now that you've got the appropriate controls for PCI DSS, you must test every one and collect evidence that each is in place and working as it should.

Even if you have done this before, you must test each control anew—your evidence must be current.

Controls will center on the security of your entire payment card transaction network: the point-of-sale system, the application that processes payment information, where and how the information is stored, security of the routers transmitting the information, how the data is encrypted, and more.

5 Gather your evidence.

In the audit world, doing a thing right is only half the battle—you also must provide documentation of your compliance.

PCI DSS is helpful for determining which evidence you will need to prove the functionality of each control.

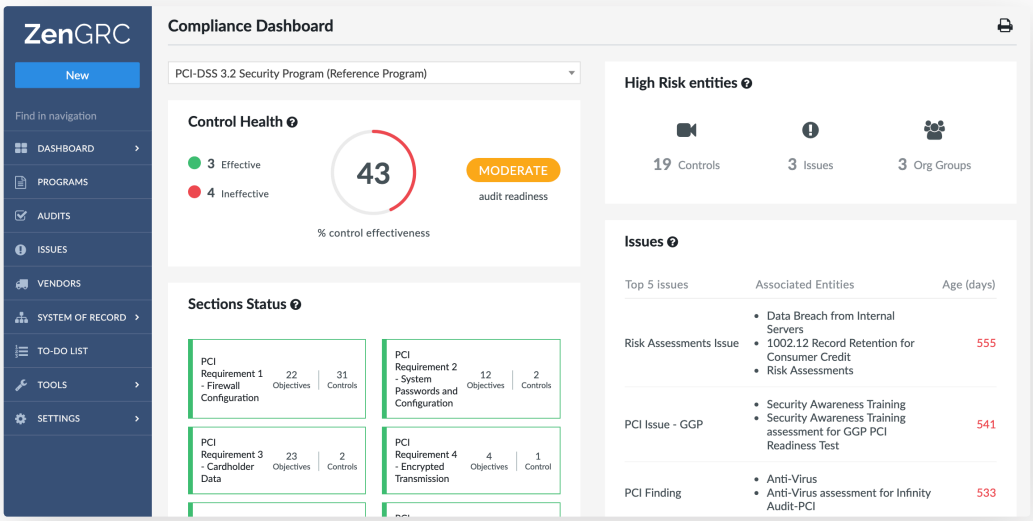
For example, the framework sets minimum requirements for password complexity. Your Active Directory may be configured to require passwords that meet the standard, but how can you prove that to an auditor? PCI DSS suggests a current screen-shot from your enterprise's Active Directory configuration showing that it requires properly complex passwords.

No Easy Task

Once you've followed these steps, you should be well prepared to pass your audit with flying colors. That's not to imply, however, that PCI DSS is a quick and easy framework to master. Its highly prescriptive nature removes much of the guesswork from compliance, but testing all your controls takes time and care, and should not be rushed.

> **Attaining PCI DSS certification could take as long as one year for smaller organizations, and up to two years for larger ones—especially if you're doing all the prep work yourself, using spreadsheets.**

Fortunately, there is a faster and easier way to prepare for a PCI DSS audit, one that saves on auditing overhead. Instead of making lists, tracking progress on spreadsheets, and searching emails and documents for evidence, why not let a quality governance, risk, and compliance software do most of the work?



ZenGRC can put your organization on the road to PCI DSS compliance by providing an overview of your compliance and risk posture on a "single source of truth" dashboard. Then, at audit time, it produces the documents required by a Qualified Security Assessor or, for enterprises with fewer transactions, performs a self-audit for you with just a few clicks. Worry-free compliance and hassle-free audits: that's the Zen way.

The Checklist

Scope

- ◯ Have you examined each of the 281 PCI DSS requirements and determined which apply to your enterprise?

Firewalls

- ◯ Does your network have a firewall between the card data environment (CDE) and the rest of the enterprise?
- ◯ Does that firewall allow only designated systems to communicate with CDE systems using approved ports?
- ◯ Does the firewall block all out-of-scope networks from communicating with your enterprise's CDE systems?

Encryption

- ◯ Do you use point-to-point encryption from the moment a cardholder submits their information all the way through payment processing?
- ◯ Have all your point-of-sale devices, software, and point-to-point encryption devices been approved by the PCI council?

Third-party compliance

- ◯ Does your organization outsource any functions in the scope of PCI DSS? Are those vendors compliant with the framework?
- ◯ Do you have written agreements with vendors establishing who is responsibility for compliance with each applicable PCI DSS requirement?
- ◯ Do you use a third party to handle your payment processing? Is that processor PCI DSS compliant?
- ◯ Do you retain any payment information from transactions? Is your payment application PCI-approved? Is it patched and up-to-date?

Segmentation

- ◯ Is your CDE segmented and isolated from the rest of your enterprise network? Have you:
  - ◯ Identified all payment channels and methods for accepting, processing, and storing cardholder information, from the point of receipt to the point of destruction, disposal, or transfer?
  - ◯ Included in this identification all systems within and connected to the CDE?
  - ◯ Implemented controls that restrict access to this segment only to those who need it?
  - ◯ Tested to be certain that in-scope and out-of-scope networks cannot communicate?
  - ◯ Ensured that cardholder data does not get transmitted via wifi?

Disposal

- ◯ Does your enterprise retain cardholder data? Why do you keep it? Do you keep only what you need?
- ◯ For how long do you retain cardholder data? Do you dispose of it as soon as you no longer need it?
- ◯ How do you destroy and dispose of cardholder data? Has your method been approved by the PCI Security Council?

Compliance

- ◯ Have you determined your enterprise's compliance with each of the objectives and sub-objectives on your list of applicable PCI DSS requirements?

Controls

- ◯ Have you recently tested each of the controls on the security of your payment transaction network to ensure that all are working as they should?
- ◯ Have you collected evidence attesting that each control is functioning properly?

About Reciprocity

Reciprocity provides ZenGRC to the world's leading companies. Our cloud-based solution with fast, easy deployment, unified controls management, and a centralized dashboard offers simple, streamlined compliance and risk management, including self-audits, without the hassle and confusion of spreadsheets. Contact a Reciprocity expert today to request your free demo, and embark on the worry-free path to regulatory compliance—the Zen way.

www.reciprocitylabs.com/resources
engage@reciprocitylabs.com
(877) 440-7971