RECIPROCITY

rethink compliance.

PCI-DSS:

Steps to Successful Scoping

PCI DSS compliance looks and feels overwhelming, even for information security professionals who have been around a while. Broken up into twelve different objectives and then various sub-steps within those original twelve, the sheer amount of information can feel like an avalanche of requirements falling on your head. However, these requirements can be scaled back by shrinking the scope of the information and locations to be reviewed. In some cases, evaluating and mitigating certain risks can minimize the scope of the overall audit.

Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.*

The first question to ask in the PCI DSS process is, "where do I need to be compliant?" Starting this process means looking at the information that the organization collects. If you're not accepting payments, then you may not need to be PCI DSS compliant. Sensitive cardholder data includes, but is not limited to, the information on the chip, the card number, the cardholder name, the expiration date, and the CAV2/CID/CVC2/CVV2 on the back of the card. More importantly, an organization should never be storing any information contained on the back side of the card or the CID. The easiest way to mitigate risk is to not accept any information. This might be unrealistic, but even if you don't store information, any area where the information is transmitted would need to be protected. This includes ensuring the security of card readers, point of sale systems, store networks and wireless access routers, payment card data stored in paper-based records, and online payment applications and shopping carts.

The next thing to determine is where the transactions occur. This means looking at the security of the POS system and the application that processes the payment information. In order to protect information at this point, buy and use only those PIN devices listed on the PCI security standards website. In addition, only use PCI validated software.

The last step would be to determine where the transaction information travels. Whenever possible, the organization should make sure to avoid storing cardholder information on individual computers or on paper. In addition, the company networks must have a firewall, and all wireless routers must be password protected and use encrypted.

Minimizing Network Scope and Risk

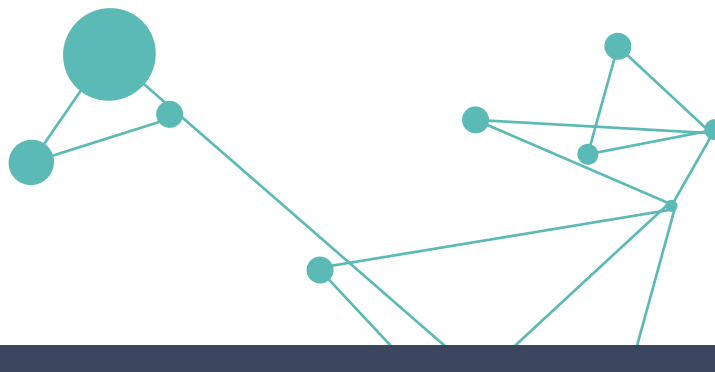
Requirement 1.1:
Establish and implement firewall and router configuration standards.

Requirement 1.2:
Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

Firewalls are one way to block access. First, they can be used to block external users from coming into your organization. Second, they can keep individuals within your organization from accessing information they do not need to have. With these controls in place, your organization begins the process of segmenting data on a need-to know basis.

In addition to firewalls, use encryption. If you're using approved methods of point-to-point encryption (P2PE), tablets, POS systems, laptops, and desktops, these methods may have reduced PCI-DSS compliance requirements. This doesn't mean that the organization is totally free of all requirements, but it can reduce some of the compliance work an organization has to perform.

Similarly, if an entity outsources in-scope functions or facilities to a third party, or utilizes a third-party service that impacts how it meets PCI DSS requirements, the entity will need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS—either for the entity or the service provider. It is also important for both parties to clearly understand which PCI DSS requirements are being provided by the service provider and which are the responsibility of the entity using the service. See PCI DSS Requirement 12.8.



Use of Third-Party Service Providers/Outsourcing

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

There are two options for third-party service providers to validate compliance:

1. Annual assessment: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or
2. Multiple, on-demand assessments: If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews with the results of each review provided to the respective customer.

For some organizations, this can remove the need for compliance entirely. For example, if your organization is small and using a third party service that handles all of your payments processing, you may need to worry less about certain aspects of PCI compliance. You will still need to ensure that you review their PCI compliance regularly, but many compliance activities will become their responsibility.

Another means of reducing PCI compliance responsibilities is to use an approved third-party payment application. By using one of the applications listed on the PCI website, the organization can avoid having to focus on application compliance. Instead, your duty is limited to ensuring that the application retains its PCI Security Council approval. Although there's still a risk associated with the third party, the risk shifts. Your organization needs to make sure that it keeps up with the software company's patches and updates. However, the risk is transferred to the extent that you do not have to continually scan for vulnerabilities in the same manner as the application's creators.

Network Segmentation

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 (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.*

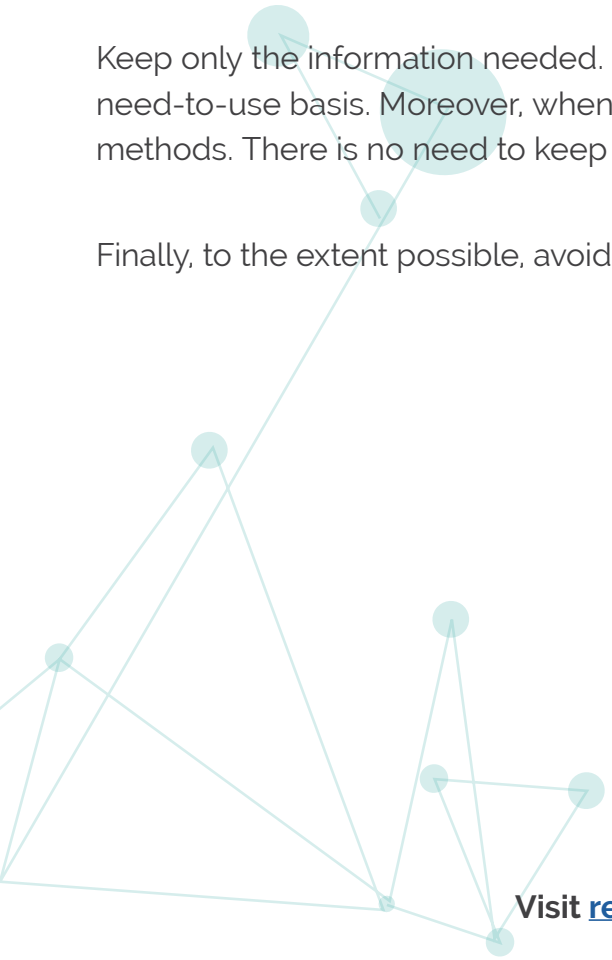
Look to segmentation to help focus the scope of the audit and risk. Segmentation starts by looking at the different people, processes, and

technologies that interact with card holder data. The next step is to put controls in place that only allow access for those who need to know it. For example, you might be using firewalls and routers to keep cardholder data from passing into or through out-of-scope networks. This means that you're protecting the data, keeping it on one path, and that one path is within the PCI DSS scope. However, it also means that the other data paths aren't in scope thus mitigating the risk for those and removing them from the audit. If you can ensure that no communication exists between in-scope and out-of-scope networks, then you have narrowed the focus of your compliance. When looking at segmentation, however, you need to make sure that you are evaluating those systems within the customer data environment and those systems connected to the customer data environment. If you are not using segmentation, then all data is within the environment and within the scope.

Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer.*

Keep only the information needed. Ensure that information, physical or electronic, is kept on a need-to-use basis. Moreover, when destroying data, ensure that you are using one of the approved methods. There is no need to keep information for a rainy day.

Finally, to the extent possible, avoid wireless transmission of information.



Visit reciprocitylabs.com to learn more.

*https://www.pcisecuritystandards.org/document_library?category=educational_resources&document=pci_scoping_guidance

Reciprocity, Inc.
2148 3rd Street
San Francisco, CA 94107

reciprocitylabs.com
(415) 851-8667
engage@reciprocitylabs.com