ZenGRC

REDUCE PCI DSS SCOPING — AND RISK

KEY WAYS TO SIMPLIFY PCI COMPLIANCE

www.ZenGRC.com

PCI DSS compliance looks and feels overwhelming — even for information security professionals who have been around a while.

Broken up into 12 different requirements and numerous sub-requirements — **281 objectives in all!** —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.

Read on to learn key methods that will not only reduce the scope of your assessment, but will also reduce your risk.

The 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) comprises 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, "What is the scope of my payments environment?" 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. However, if you process, store or transmit cardholder data (CHD), you will be responsible for performing some type of annual assessment and attestation.

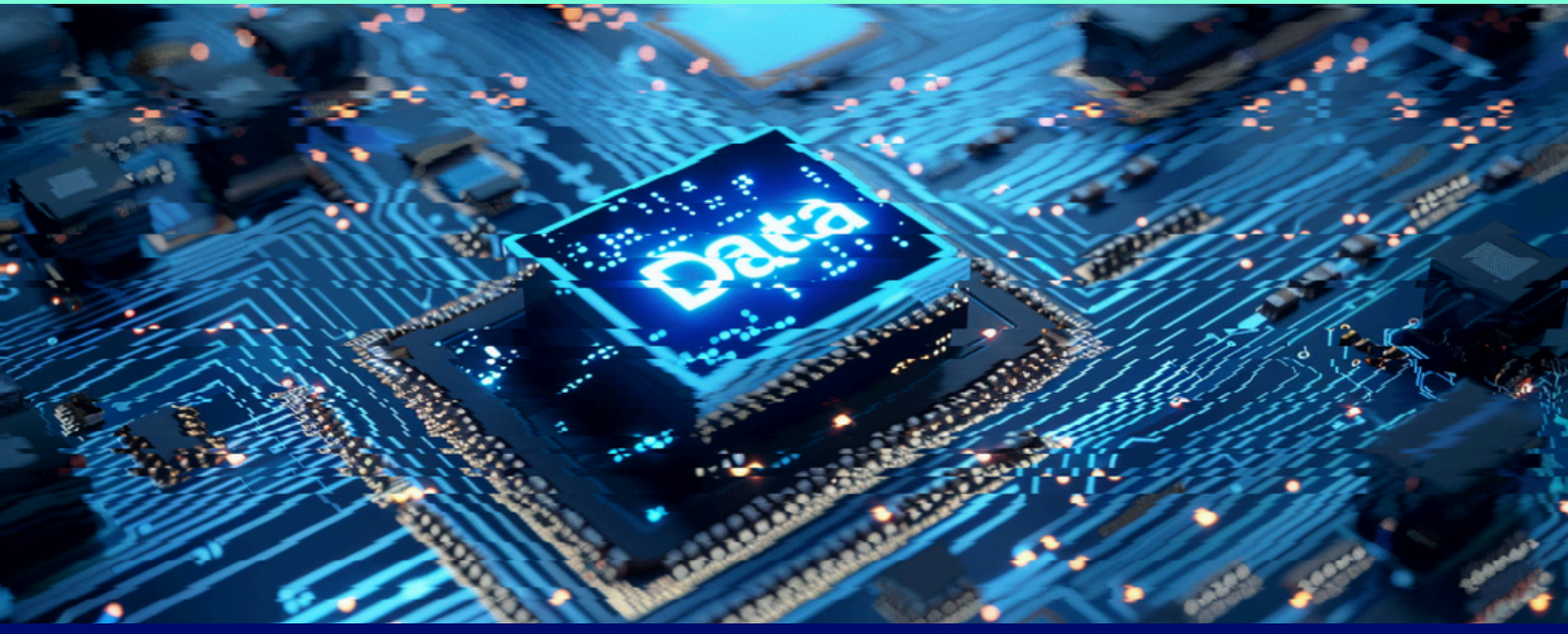
To determine the scope of your payments environment, document the data flow of the different ways your organization accepts credit card payments. Be sure to include all of the steps to ensure that you have an accurate picture of your process.

The resulting data flow diagram will help you to identify the networks and systems that are in-scope for your PCI program.

Sensitive cardholder data includes, but is not limited to, the information on the chip, the card number, the cardholder name, the expiration, and the CAV2/CID/CVC2/CVV2 on the back of the card. It's important to note that some of these data elements should never be stored in an organization's environment.

The surest way to mitigate risk is to not accept any information in your own environment. The easiest way to do this is to outsource most of the payment acceptance process to a third party. 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.

Once you have determined the scope of your CDE, you can look for opportunities to reduce the scope of your PCI assessment.



Minimizing Network Scope and Risk

An entity may 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 networks, and is also used to segment an out-of-scope network.*

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.

Another way to reduce the risk to and the assessment scope of your environment is to leverage encryption technologies. If you're using approved methods of point-to-point encryption (P2PE), many information assets (POS devices, computers, etc.) may be exempt from portions of your PCI assessment. This doesn't mean that the organization is exempt from these requirements, but it can reduce some of the compliance work an organization has to perform.

Outsourcing some or most of the payments process can also reduce the scope of your assessment. This transfers responsibility for the assessment of certain requirements to the service provider performing the outsourced processes. It is 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. It is also important to note that ultimately the merchant is responsible for ensuring the compliance of the third party processing payments on their behalf (see PCI DSS Requirement 12.8). The PCI Security Council has anticipated these types of joint-processing agreements and provided Self-Assessment Questionnaires (SAQs) to facilitate assessing such environments in some cases.

Reducing Risk with 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)
- A "flat network" — without adequate network segmentation (a.k.a. a flat network), the entire network is in scope of the PCI DSS assessment.*

One of the most effective ways of reducing the risk to your CDE and the scope of your PCI assessment is to use network segmentation to isolate your CDE from other networks. 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 it to perform their job duties.

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 removing them from the scope of the assessment. If you can ensure that no communication exists between in-scope and out-of-scope networks, then you have narrowed the focus of your assessment.

When looking at segmentation, however, you need to make sure that you are evaluating those systems within the cardholder data environment and those systems connected to the cardholder data environment. If you are not using segmentation, then all data is potentially within the cardholder data environment and within the assessment scope.

Another important way to reduce risk to your CDE and to reduce the scope of your assessment is to only store the CHD needed to perform transactions. This is another area where outsourcing payment transactions can reduce the scope of your assessment. In such cases, it typically becomes unnecessary to store any CHD in your environment. However, if it is absolutely to store CHD for business purposes, ensure that the information is protected using the requirements in the PCI-DSS and that once this data is no longer needed, it is destroyed using approved data destruction methods.

WE GET IT.
Assessing your PCI environment can seem like a daunting task. But by using methods to reduce the scope of your assessment, you can simplify the process and, ultimately, reduce your risk.

WE CAN ALSO HELP. ZenGRC's fully integrated and automated ZenGRC platform helps you navigate the PCI maze and identify and resolve your gaps. ZenGRC is continually updated as PCI changes occur and alerts you when it's time to re-audit. You can then generate reports within ZenGRC to demonstrate your compliance.

In other words, no more messy spreadsheets. No more confusion. And, most important, no more worries about PCI DSS compliance.

To learn more about how ZenGRC can help you drive greater PCI compliance efficiencies with less effort, visit us here

About ZenGRC

ZenGRC is powering the next generation of information security with the fastest, easiest and most prescriptive solutions in the market. ZenGRC delivers a full catalog of compliance, risk and other infosec applications through one simple user interface that drives greater transparency, actionable insights and benchmark reporting.

Recognized for its GRC expertise and its accelerated time-to-value, ZenGRC is transforming risk and compliance from a cost-center to a value-creator for businesses across the globe. ZenGRC is headquartered in San Francisco.

www.ZenGRC.com
engage@ZenGRC.com
(877) 440-7971