



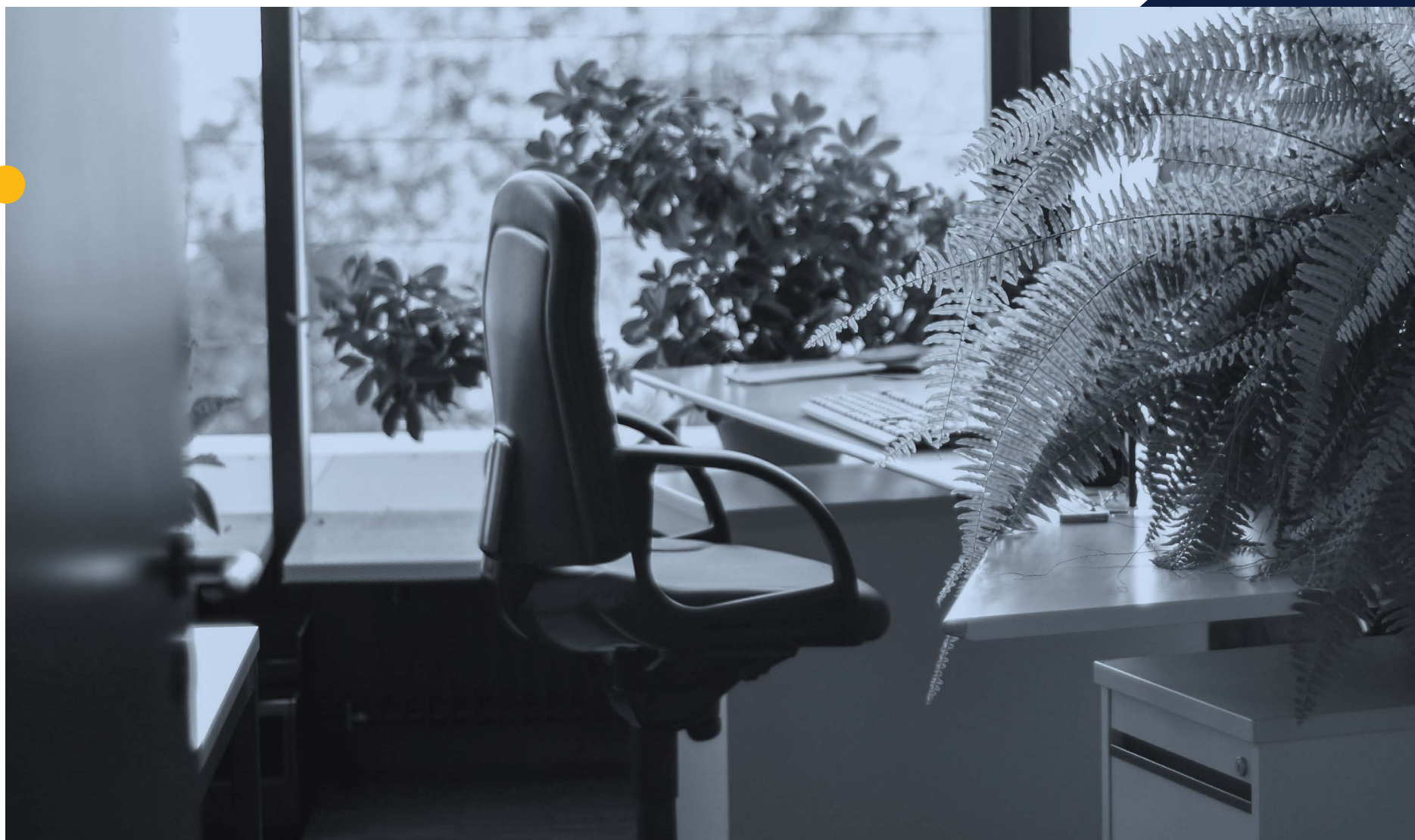
SIMPLIFY PCI COMPLIANCE.
REDUCE PCI SCOPE.



T A B L E O F C O N T E N T S





VIA POINT-TO-POINT ENCRYPTION (P2PE)	19
BY LIMITING WHO CAN SEE CREDIT CARD DATA	20
BY LIMITING ACCESS TO CREDIT CARD DATA	21
BY LIMITING CARDHOLDER DATA IN PHYSICAL LOCATIONS	22
VIA SECURE ONLINE PAYMENTS	23
VIA TOKENIZATION	24
VIA OUTSOURCING	25
THE US SIGNAL ADVANTAGE	26





If your company handles cardholder data in any way, compliance with the PCI Data Security Standard (PCI DSS) is mandatory. It can also be time-consuming and expensive — particularly for PCI DSS v.4.0, which was released March 31, 2022 and goes into effect March 31, 2024.

Even if you outsource some or all of your IT resources and assets, you can't hand off the responsibility for PCI compliance to a third-party vendor. A vendor may be able to help you meet certain compliance requirements. However, the responsibility for PCI compliance resides solely with your company.

There is a way to at least alleviate some of the compliance burden. That's by shrinking the footprint of your cardholder data environment.

In this eBook, we'll discuss how to determine your scope for PCI compliance and ways to possibly reduce it to simplify the entire compliance process.

MINIMIZE YOUR CARDHOLDER **DATA FOOTPRINT**



KNOW WHAT'S IN SCOPE

All components of your cardholder data environment — specifically anything or anyone that touches and/or sees cardholder data — is in scope for PCI compliance.

To determine the exact extent of that scope and what must be included for PCI compliance, identify:

YOUR CARDHOLDER DATA ENVIRONMENT

Your cardholder data environment includes the people, processes, and technology that handle cardholder data or sensitive authentication data.

ALL SYSTEM COMPONENTS THAT ARE LOCATED WITHIN OR CONNECTED TO THE CARDHOLDER DATA ENVIRONMENT

System components are the wired and wireless network devices, servers, computing devices, and applications. Also included are any systems, that if compromised, could affect your cardholder environment. Note: virtualization components, such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors, are also considered system components within PCI DSS.

ALL FLOWS OF CARDHOLDER DATA AND THE LOCATIONS INVOLVED

All types of systems and locations should be considered as part of the scoping process. This includes backup and recovery sites, as well as any failover systems.

THE WHO AND/OR WHAT

This refers to who and/or what can initiate a connection to any of the systems that handle cardholder data.

You'll need to perform this scoping exercise at least annually and prior to your annual PCI assessment.



In the process of identifying where cardholder data resides or passes through, don't just look to the usual places.

**SEARCH BEYOND THE
EXPECTED**

Consider secondary systems, such as log servers and systems that reside outside of the typical card data environment, such as DNS. Do they touch cardholder data in anyway? If yes, they're in scope.

Where else should you look? If you access a web page for data entry, cardholder data may be found in temporary browser cache files.

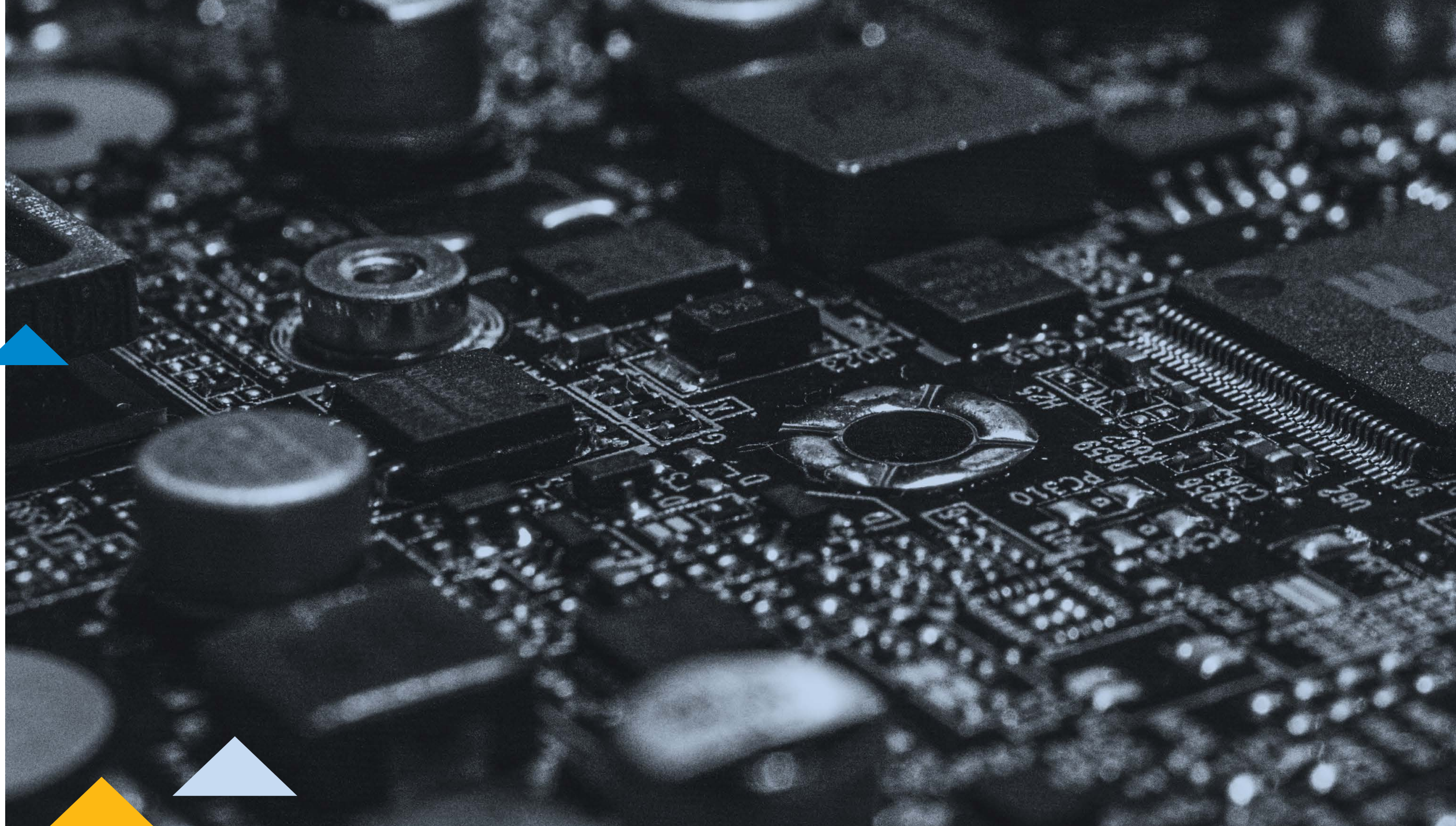
While it is up to the website developer to make sure the website doesn't store cookies or temporary log files with sensitive data, you may not have full control of your website. It's just one more reason to thoroughly evaluate all possible systems for cardholder data.

There may also be processes that you aren't aware of that touch cardholder data. For example, retail store and call center

employees may write down card numbers manually for phone orders, when power outages occur or when orders come in via email.

While your company's databases may be programmed to encrypt all cardholder data, the servers may still hold temporary files, log files, or back-ups with unencrypted data. Or, you may have other departments within your organization that have post-transaction processes that use cardholder data. They all count in your PCI scope. One way to locate unencrypted card data is to run a card discovery tool.





WHO'S TALKING TO
YOUR SYSTEMS



Do you know everything and/or everyone that can communicate with your organization's IT systems?

Carefully assess all your processes.

- + Who has permission to access your card data?
- + How do you transmit that data?
- + How do you log in to your systems?
- + How are your systems backed up?
- + How do you reset passwords?
- + If you have a server that handles cardholder data, what else talks to it?

Anything that can connect to an in-scope server that handles cardholder data is in your scope for PCI compliance.

To get systems out of scope, your defined in-scope servers should only be communicating outbound to specific destinations for the data or services they need. Do not let other systems access in-scope servers.



Here's an example of a typical PCI scoping exercise. You can use this as a starting point for determining your company's PCI scope.

ACTIVITY

Identify how and where your company receives cardholder data.

Locate and document where account data is stored, processed, and transmitted.

Identify all other system components, processes, and personnel that are in scope.

DESCRIPTION

Identify all payment channels and methods for accepting cardholder data from the point where the cardholder data is received through to the point where it's destroyed, disposed of or transferred.

Identify the people, processes, and technologies involved in storing, processing, and/or transmitting cardholder data. Document all cardholder data flows.

Identify all business and technical processes, system components, and people that can or do interact with or influence the cardholder data environment.

EXAMPLE 1:

SAMPLE PCI SCOPING EXCERCISE



(EXAMPLE 1 CONTINUED)

ACTIVITY

Implement controls to minimize scope to necessary components, processes, and personnel.

Implement all applicable PCI DSS requirements.

Maintain and monitor.

DESCRIPTION

Implement controls to limit connectivity between your cardholder data environment and other in-scope systems to only what is necessary. Implement controls to segment your cardholder data environment from any people, processes, and technologies that don't need to interact with or influence the cardholder data environment.

Identify and implement PCI DSS requirements as applicable to the in-scope system components, processes, and people.

Implement processes to ensure the PCI controls remain effective every day. Ensure the in-scope people, processes, and technologies are accurately identified when changes are made.

Example 2 shows how to document your cardholder data environment, the systems connected to it or that could affect it in some way, and your out-of-scope systems. You can use any documentation and evaluation method that works best for your organization in determining your PCI scope.

SYSTEM TYPE	DESCRIPTION	SCOPE & APPLICABILITY
Cardholder data environment systems	This system component stores, processes, or transmits cardholder data/sensitive authentication data...or is on the same network segment.	These systems: <ul style="list-style-type: none"> + Are in scope for PCI DSS. + Must be evaluated against all PCI DDS requirements to determine the applicability of each requirement.

EXAMPLE 2:

DOCUMENTING WHAT'S IN AND OUT OF PCI SCOPE

(EXAMPLE 2 CONTINUED)**SYSTEM TYPE****DESCRIPTION****SCOPE & APPLICABILITY**

Systems connected to the cardholder data environment or that could affect it

This system component is on a different network (or subnet or VLAN) but can connect to or access the cardholder data environment ...or it can connect to or access the cardholder data environment via another system.... or it can impact configuration or security of the cardholder data environment, or how cardholder data/sensitive authentication data is handled— for example, a web redirection server or name resolution server...or it provides security services to the cardholder data environment—for example, network traffic filtering, patch distribution, or authentication management...or it supports PCI DSS requirements, such as time servers and audit log storage servers...or it provides segmentation of the cardholder data environment from out-of-scope systems and networks—for example, firewalls configured to block traffic from untrusted networks.

These systems:

- + Are in scope for PCI DSS. Even where a connection is limited to specific ports or services on specific systems, those systems are included in scope to verify that the applicable security controls are in place.
- + Must be evaluated against all PCI DSS requirements to determine the applicability of each requirement.
- + Must not provide an access path between cardholder data environment systems and out-of-scope systems.

SYSTEM TYPE

DESCRIPTION

SCOPE & APPLICABILITY

Out-of-scope systems

This system component doesn't store, process, or transmit cardholder data/sensitive authentication data....and it isn't on the same network segment or in the same subnet or VLAN as systems that store, process, or transmit cardholder data.... and it can't connect to or access any system in the cardholder data environment...and it can't gain access to the cardholder data environment or affect a security control for cardholder data environment via an in-scope system....and it doesn't meet any criteria described for connected-to or security-impacting systems, per above.

Note: These systems are not in scope for PCI DSS but could still represent a risk to the cardholder data environment if they aren't secured. It is strongly recommended that security best practices be implemented for all out-of-scope systems/networks.

These systems:

- + Are not in scope for PCI DSS; therefore, PCI DSS controls are not required.
- + Have no access to any cardholder data environment system; if there is any access, then system is in scope.
- + Are considered untrusted (or "public")—there is no assurance they have been properly secured.

If on the same network (or subnet or VLAN) as, or otherwise has connectivity to, a connected-to or security impacting system, controls must be in place to prevent the out-of-scope system from gaining access to the cardholder data environment via the in-scope systems. These controls must be validated annually at a minimum.

Once you know the full extent of your PCI scope, you can begin determining ways to reduce it. Here are a few to consider:

- + Network segmentation
- + Point-to-point encryption
 - + Limit access to specific credit card data
 - + Limit who can see credit card information
 - + Limit card data in physical locations
- + Secure online payments
- + Use tokenization
- + Outsource

This is by no means an exhaustive list. The ways that work best for your organization will depend on your specific cardholder data environment and systems.

OPTIONS FOR **SCOPE REDUCTION**



It takes a lot of effort and time to secure all your networks instead of just the ones containing cardholder data.

Keep the networks that handle card data separate from the ones that don't by employing network segmentation. You can do this by installing firewalls between networks.

Establishing a firewall between a secure payment zone and the rest of the day-to-day business traffic can help ensure that only known and trusted sources can access the cardholder environment. This limits the size of the cardholder environment, and potentially reduces PCI scope.

If you use network segmentation, the PCI DSS requires that penetration-testing procedures must confirm segmentation is operational and isolates all out-of-scope systems from systems in the cardholder data environment.

Firewalls should also be configured to filter both inbound and outbound traffic. If an attacker gets into a system, outbound firewall rules can make it difficult to export stolen data.

PCI SCOPE REDUCTION VIA NETWORK SEGMENTATION

Point-to-point encryption technology eliminates the need for segmentation if you employ a validated point-to-point encryption solution.

Point-to-point encryption ensures that card numbers are encrypted from first card swipe at the point-of-sale and while in transit all the way to the payment processor. If you only use point-to-point encryption to process credit cards, your entire merchant network is out of scope.

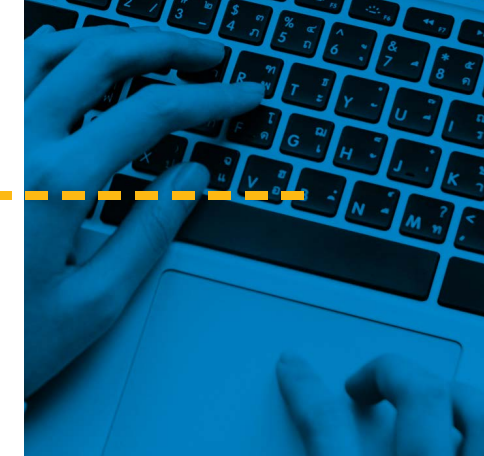
Among the considerations: encryption keys can be used for many purposes, whether it is to encrypt SSL connections or encrypting

sensitive data. When using keys to encrypt data, keeping private keys protected on servers and putting together a key management policy is required that considers how keys are used, rotated, managed, and secured. This will help protect data that does need to be stored or transmitted through merchant systems.

Using a third-party service provider for point-to-point encryption is also an option. This eliminates most PCI requirements as the service provider is responsible for securely handling cardholder data.

PCI SCOPE REDUCTION

VIA POINT-TO-POINT ENCRYPTION (P2PE)



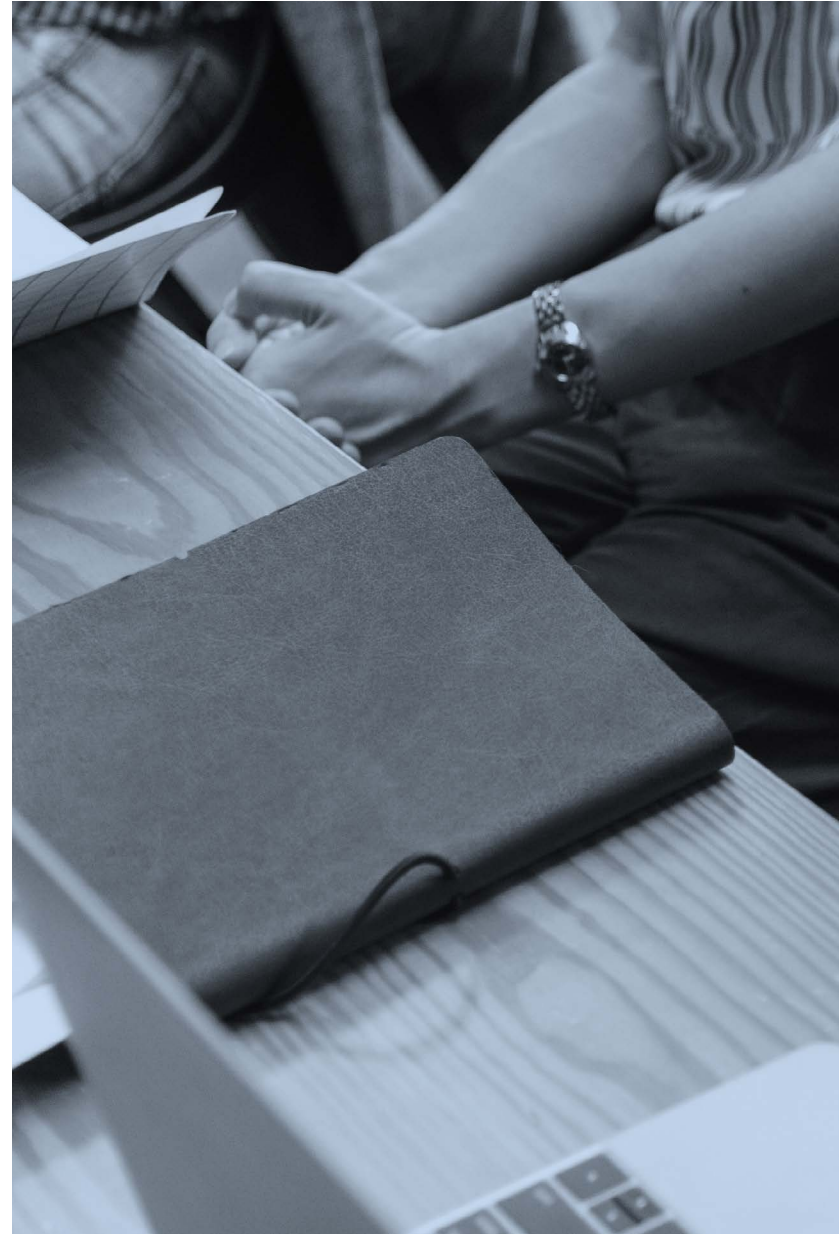
Simply reducing the number of people within your organization that can see cardholder information can reduce your PCI scope.

If certain employees don't require access to the data, there is no reason they should ever see it. You can limit who can see cardholder data by ensuring that it is only shared on specific protected networks, separate from other information that various departments typically access. Network segmentation can help with this. For extra security, the data should also be encrypted at rest and in transit.

Under PCI DSS 3.2, the latest version as the standard as of the publication date of this eBook, greater access controls are now in place for system administrators.

Any personnel with administrative access into environments that handle cardholder data must use multi-factor authentication. A password alone is no longer enough.

This extra layer of authentication provides additional assurance that anyone attempting to gain access to cardholder data are who they claim to be. The use of multi-factor authentication also makes it more difficult for cyber attackers who would need to compromise at least two different authentication mechanisms.



PCI SCOPE REDUCTION BY LIMITING WHO CAN SEE CREDIT CARD DATA



PCI SCOPE REDUCTION BY

LIMITING ACCESS TO CREDIT CARD DATA

Just as you can limit who sees cardholder data, you can limit access to specific kinds of cardholder data.

There may be people within your organization who need access to certain kinds of cardholder data to do their jobs. For example, your marketing department may need access to specific kinds of cardholder information to analyze customer buying patterns. Likewise, your technical support staff may require certain kinds of cardholder data to verify customers' identities. That doesn't mean they need to be able to access all cardholder data.

To reduce PCI scope, limit access to only the specific types of cardholder data that are required by the various types of employees who require it to do their jobs. You can further truncate cardholder data to whatever extent allows only certain kinds of information to be accessed.

Not surprisingly, cardholder data is at high risk in most retail and other physical environments where credit cards are used.

Encryption of credit card data at the point of purchase will minimize your physical PCI footprint. If you can eliminate credit card data from the purchasing process altogether, you can avoid four of the twelve PCI requirements:

REQUIREMENT 1 - Install and maintain a firewall configuration to protect cardholder data. If cardholder data isn't stored in the environment, a dedicated firewall isn't required to protect it.

REQUIREMENT 3 - Protect stored cardholder data. The responsibility of protecting cardholder data would reside with the third-party vendor if the data resides its environment instead of yours.

REQUIREMENT 4 - Encrypt transmission of cardholder data across open, public networks. The third-party vendor would encrypt the data at the point of payment and be responsible for transmitting it across a secure network.

REQUIREMENT 9 - Restrict physical access to cardholder data. If cardholder data is stored with a third-party vendor, your employees will no longer be able to physically access it.

PCI SCOPE REDUCTION BY LIMITING CARDHOLDER DATA IN PHYSICAL LOCATIONS

Another way to reduce PCI scope is to employ transparent data redirection when accepting online payments.

They are especially useful in healthcare organizations that accept patient web payments through electronic health records (EHR) software.

Using the API, a patient's credit card information is sent directly to a third-party processor, and never passes through the healthcare organization's web server. This reduces the PCI scope on that server.

PCI SCOPE REDUCTION
VIA SECURE ONLINE
PAYMENTS

Tokenization is the process of swapping highly sensitive cardholder data for a ‘token.’

The token has several random digits that can't be restored back to their original value. This helps ensure that the sensitive information is kept safely in one place. By reducing where cardholder data is located, the scope of your PCI audit is greatly reduced.

Just make sure that if you use tokenization, you're still not storing primary account numbers or storing old caches of primary account numbers in your environment. Run data discovery tools to find all primary account number caches so you can replace them with a token. Anytime you remove primary account numbers from your environment, you reduce your compliance risks.

Using a third-party vendor that uses tokenization also eliminates cardholder data from being stored in your environment, shrinking your PCI scope. However, you are still ultimately responsible for PCI compliance. It's up to you to make sure any vendor you work with is safeguarding cardholder data sufficiently and meets the PCI requirements.

PCI SCOPE REDUCTION

VIA TOKENIZATION





Yet another way to reduce PCI scope is to outsource various IT-related tasks and responsibilities to third parties.

This can include anything from firewall management to system hosting to data storage. For a predictable monthly fee, you eliminate some of the stress of PCI compliance while also freeing up your internal IT resources for other endeavors. The key is to work only with vendors that are themselves PCI compliant. Always ask to see certifications and inquire about the various security protocols in place.

Even if you work with a third-party vendor that puts your entire cardholder data environment in a “PCI-compliant” cloud, you’re still responsible for overall PCI compliance and for drafting a Report on Compliance (ROC). The benefits of working with a PCI-compliant cloud services provider is that you get the secure architecture and supporting security management practices that can help you meet some of your compliance requirements. In many cases, the vendor can work with you and your auditors to answer questions and provide necessary documentation.



PCI SCOPE REDUCTION

VIA OUTSOURCING

Working with a third-party provider that provides compliant, audit ready IT infrastructure — like US Signal — can help ease some of your organization's compliance burden. US Signal takes pride in going beyond both the norm and requirements in our industry to maintain a well-governed, high quality infrastructure.

THE US SIGNAL
ADVANTAGE

Here are just a few advantages we offer through our compliant IT solutions:

- + Cloud infrastructure and data centers independently audited to meet SSAE 18, SOC 1, Type 2, SOC 2, Type 2, HIPAA/HITECH, GRPR Privacy Shield, International Traffic in Arms Regulations (ITAR), FBI CJIS, and PCI-DSS.
- + People-centric security with all US Signal employees trained at hire and annually on security policies and protocols.
- + Risk-based BC/DR plan that includes multiple live tests each year, follow-up action item review, and reporting.
- + Full Governance, Risk, and Compliance (GRC) program.
- + Audit-ready IT environments with technical and security controls to meet a variety of regulatory requirements and industry standards including: Sarbanes-Oxley, FDA, Gramm-Leach-Bliley, ITAR, and FISMA.
- + Vendor due diligence program, executive-level security team, internal audit program following ISO-19011, and other strategies to optimize service availability while mitigating MSSP risks.
- + Audit assistance including helping with management representation letters and regulatory questionnaires and providing a signed Business Associate Agreement (BAA) or copies of compliance documentation.
- + On-staff compliance officer.
- + Extensive experience working with customers in retail, financial services, and other industries that must comply with PCI DSS.

To learn how US Signal can help lessen your company's PCI compliance burden, call us at 866.2. SIGNAL or email: info@ussignal.com.