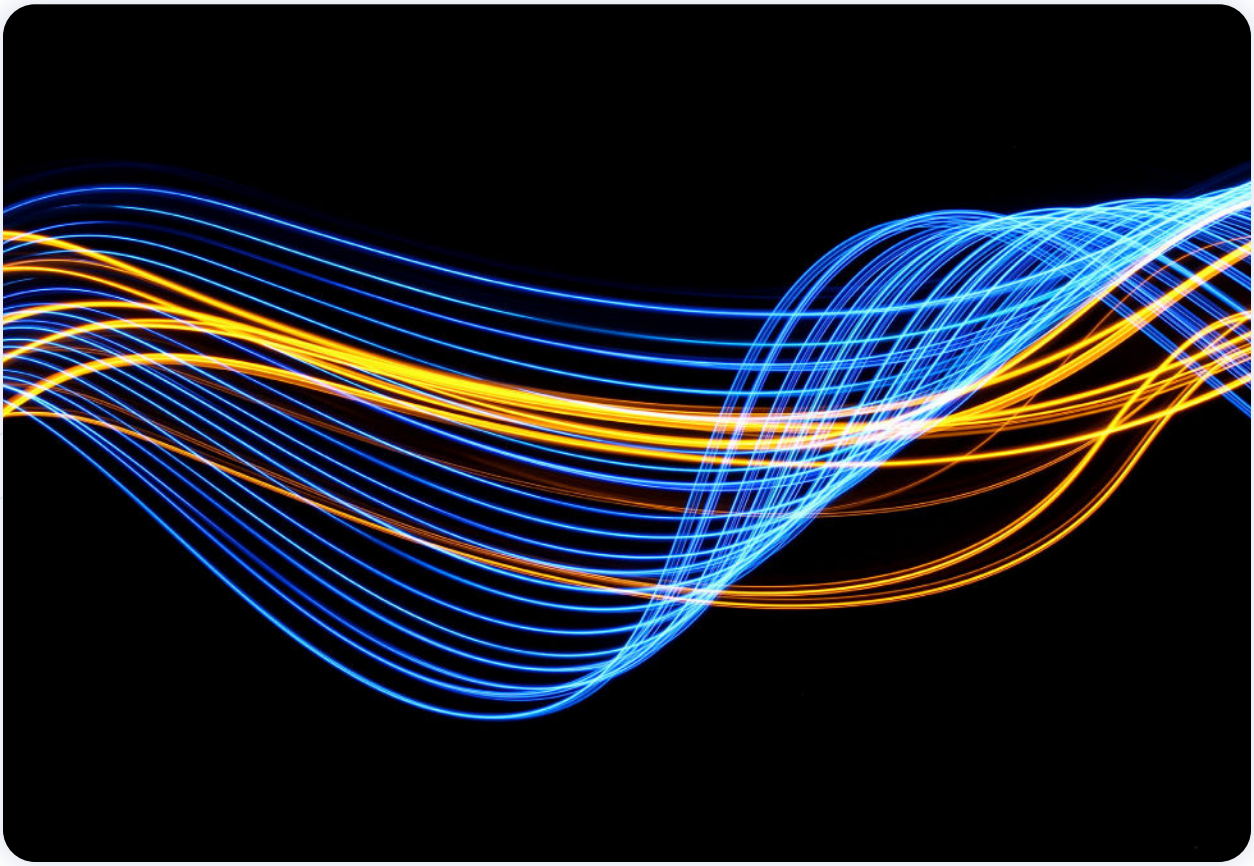


tokenex

PCI DSS Compliance Guide

How cloud security can reduce PCI scope and simplify the compliance process

The PCI problem

If your organization is responsible for the processing, storage, or transmission of cardholder data, you are likely aware of the Payment Card Industry Data Security Standard, if not painfully familiar with its many requirements. Or, if you're new to the space—maybe you just began accepting a new form of payment or your business has outgrown its current level of PCI compliance—you're probably wondering how to make sense of these dense regulatory obligations.

Regardless of your reason for seeking compliance or your existing knowledge of the process, TokenEx can help. In this guide, you'll find initial steps and strategies for reducing the complexity and cost of compliance—and ultimately achieving it.

To best become PCI compliant, we recommend a method called "descoping," which we'll explain in detail here. Our preferred descoping technique involves a data-centric approach to protecting cardholder data that leverages a cloud security platform to remove sensitive data from your internal systems and safely store it outside of your environment.

The benefits of descoping

Reduce the financial cost associated with PCI DSS audits

Expedite the PCI compliance process

Decrease the amount of effort required to maintain compliance

Diminish the impact of a potential data breach

Strategies for scope reduction

The scope of an organization's environment is the extent to which payment card data exists within its systems, so any portion of a network that stores, processes, or transmits that data is within scope. With this in mind, descoping is the process of reducing the breadth of compliance by minimizing the amount of people, processes, and technology that interact with cardholder data.

To determine which areas of your internal systems are within scope, you can create a data flow that maps how payment data travels through your environment. From there, you can see who and what is interacting with cardholder data and where those interactions are occurring. In the process, you will identify which assets along the data flow are in scope and therefore need to be examined to ensure security and compliance.

Organizations can reduce the scope of a cardholder data environment in several ways. For example, they can limit the number of employees allowed to access sensitive card data. They can store the data in a portion of their network that's isolated from the rest, which is known as segmentation. Additionally, they can use only technologies or third-party services that either are PCI compliant or don't interact with cardholder data.

Terms to know

Scope

The extent to which payment card data exists within an organization's systems—any portion of a network that stores, processes, or transmits that data is in scope.

Descoping

Minimizing the people, processes, and technology that interact with cardholder data. This reduces the scope of compliance by removing sensitive data from an organization's environment.

Need a full list of compliance terms? Check out the glossary by clicking here.

Glossary

Many organizations utilize a combination of segmentation and encryption to achieve PCI compliance, but each of these strategies presents its own set of challenges—not to mention the overhead required to execute, monitor, and maintain them internally. Fortunately, tokenization has emerged as a simpler scope-reducing alternative that can preserve business intelligence while minimally disrupting vital operations. Specifically, the TokenEx Data Protection Platform is a tokenization technology that can help reduce overhead and better position organizations to meet future regulatory compliance obligations.

Tokenization is the process of converting sensitive data into nonsensitive, mathematically unrelated data called tokens. Once a value is tokenized, it is no longer considered cardholder data, so a placeholder token can flow through your environment without bringing any of the elements that store, process, or transmit it into scope. Cloud-based tokenization even outsources the handling of sensitive payment information to security experts, further reducing compliance and operational costs while mitigating the risk and liability associated with a potential data breach.

Ideally, tokenization occurs outside of your environment so cardholder data in its original, sensitive form is never introduced. If this is the case, organizations can virtually remove their networks from scope and greatly increase the likelihood that they'll be able to maintain compliance between annual assessments.

Terms to know

Segmentation

The process of segmenting or isolating the portion(s) of a network that contain cardholder data from the rest of an organization's internal systems.

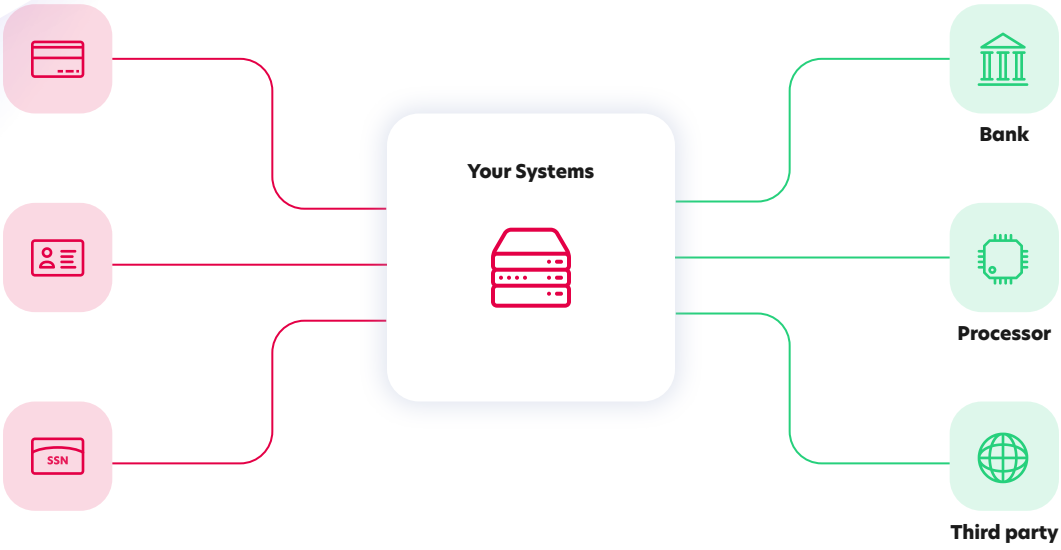
Encryption

The process of obfuscating data by encoding it with a mathematical key.

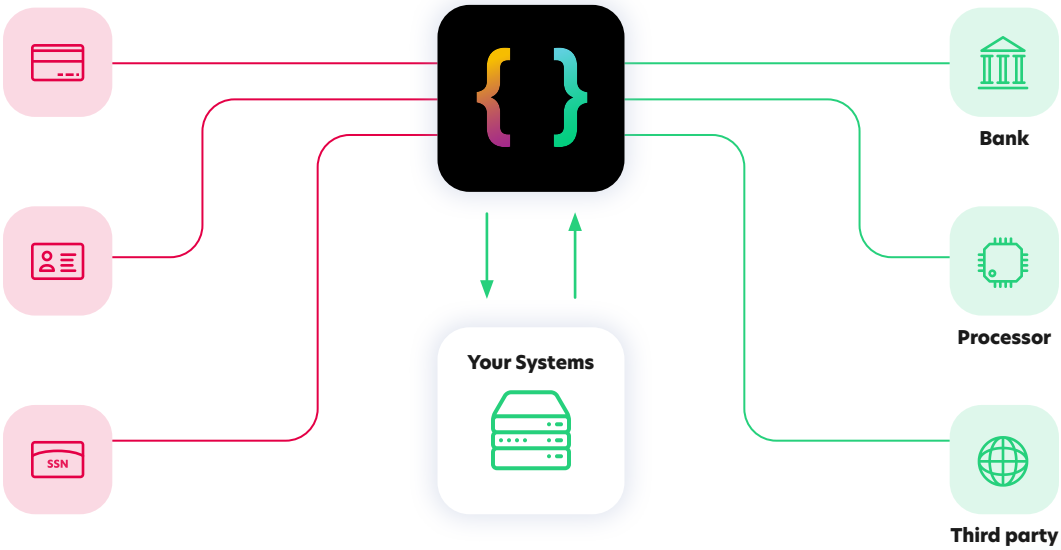
Tokenization

The process of converting sensitive data into nonsensitive placeholders—mathematically unrelated data called tokens.

Before and after Tokenization



All cardholder data that passes through your internal systems in its unprotected form is subject to PCI DSS compliance. The diagram above shows a flat network that is entirely within PCI scope.



TokenEx's Cloud Security Platform captures sensitive cardholder data from your customers at the point of acceptance, secures and desensitizes it via tokenization, and then passes it along to your desired endpoint. This reduces the scope of PCI compliance by removing cardholder data from your organization's environment.

Compliance types

As valuable as descoping can be, it alone does not equate to compliance. In order to become compliant, an organization must prove it has met all PCI DSS requirements, either on its own or with the assistance of third-party providers. Depending on the state of an organization's environment, it might qualify for a self-assessment or require an external audit from a qualified party.

A variety of factors can impact the scope, cost, and complexity of compliance. Ideally, an organization would be able to reduce its scope to a level sufficient to qualify for a self-assessment questionnaire (SAQ). SAQs, in effect, enable organizations to audit themselves without working with—or paying for—a qualified security assessor (QSA).

E-commerce or mail-order/telephone-order merchants who outsource all cardholder functions to validated third-parties are eligible for an SAQ A or an SAQ A-EP. An SAQ A contains 22 controls, compared to the more than 300 controls for the full PCI DSS. This represents the maximum scope reduction available with cloud-based tokenization. For a full list of SAQ types, see the next page.

An SAQ A contains 22 controls. The full PCI DSS has more than 300.

SAQ Types

A

Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*

A-EP

E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*

B

Merchants using only:
• Imprint machines with no electronic cardholder data storage; and/or
• Standalone, dial-out terminals with no electronic cardholder data storage.
Not applicable to e-commerce channels

B-IP

Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
Not applicable to e-commerce channels.

C-VT

Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.
Not applicable to e-commerce channels.

C

Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.
Not applicable to e-commerce channels.

P2P-HW

Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage.
Not applicable to e-commerce channels.

D

SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.

SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Qualifying for an SAQ A

Because SAQs enable organizations to self-evaluate their environments, they represent the ideal validation tool for simplifying the compliance process. Additionally, as described below, meeting the requirements of an SAQ can help reduce the risk and impact of a potential breach.

- *Use a hosted iFrame or payments page provided by a validated service provider to capture and tokenize CHD*
- *Do not transmit, process, or store CHD via any other acceptance channel*
- *Utilize the payment services of a tokenization provider to process transactions*
- *Maintain appropriate policies and procedures*

The goal of many PCI service providers is to capture cardholder data as early as possible within acceptance channels to keep it from ever entering an organization's systems. If that card number never touches your environment, your environment essentially is removed from scope.

However, even if you outsource all cardholder data to a PCI service provider, some compliance obligations remain. For example, the controls concerning people and processes (requirements 2, 8, 9, and 12) will still apply to your organization. You can see this illustrated in the chart on the following page, which shows the scope of a flat network, segmented environment, and fully tokenized environment.

Not all organizations can qualify for an SAQ, but most can significantly reduce scope via cloud tokenization.

Compliance controls for common network types

		Flat	Segmented	Tokenized
1	Install and maintain a firewall configuration to protect cardholder data	●	◐	●
2	Do not use vendor-supplied defaults for system passwords and other security parameters	●	◐	◒
3	Protect stored cardholder data	●	◐	●
4	Encrypt transmission of cardholder data across open, public networks	●	◐	●
5	Use and regularly update anti-virus software or programs	●	◐	●
6	Develop and maintain secure systems and applications	●	◐	●
7	Restrict access to cardholder data by business need to know	●	◐	●
8	Assign a unique ID to each person with computer access	●	◐	◒
9	Restrict physical access to cardholder data	●	◐	◒
10	Track and monitor all access to network resources and cardholder data	●	◐	●
11	Regularly test security systems and processes	●	◐	●
12	Maintain a policy that addresses information security for all personnel	●	◐	◒

Tokenized example based on controls for SAQ A.

Descoping for forward-thinking compliance

By leveraging the TokenEx Data Protection Platform to tokenize sensitive cardholder data and remove it from your environment, your organization can minimize the cost, complexity, and effort of achieving and maintaining PCI compliance. Our platform was designed by two former QSAs for this exact purpose, and it represents the true value of our solution.

Additionally, we provide you with the freedom and flexibility to integrate with nearly any third party and send data to any API endpoint, enabling you to entrust your most sensitive data to security and compliance experts while promoting operational efficiency and positive business outcomes.

We understand that every organization's environment and journey to PCI compliance is different, and we recognize that descoping is not the only option for achieving it. However, this efficient and effective method uses proven techniques for segmentation and data minimization to isolate sensitive data, to store only what is absolutely necessary, and to protect what must be stored in a manner that virtually eliminates the risk of data theft.

To learn more about descoping, cloud security, tokenization, or any other topic related to PCI compliance, contact us today at *info@tokenex.com*. We'd love the opportunity to further explain how our solution can alleviate your PCI compliance pain points.}

Reduce PCI scope

Begin the compliance process today!

Request a free demo

Glossary

Self-Assessment Questionnaire (SAQ) – validation tool intended to assist merchants/service providers who are permitted by the payment brands to self-evaluate their compliance with the PCI DSS.

Report on Compliance (ROC) – a form that must be completed by merchants and service providers not eligible for an SAQ. The ROC is used to verify that the merchant being audited is compliant with the PCI DSS. The ROC must be filled out by a qualified security assessor (QSA) who has audited the merchant.

Attestation of Compliance (AOC) – a form that must be completed by a QSA or merchant (if merchant internally audits) as a declaration of the merchant's compliance status with the PCI DSS.

Approved Security Vendor (ASV) – an approved external entity that scans organizations' networks to search for vulnerabilities.

Qualified Security Assessor (QSA) – an individual employed by a QSAC (which is an organization that specifically performs PCI audits) who is responsible for evaluating CDEs.

Internal Security Assessor (ISA) – an individual within your organization who can complete SAQs and otherwise assist with PCI compliance.

Return