{tokenex} Preparing for Your PCI Audit: Tips and Checklist

There are about 300 sub-requirements in the PCI Data Security Standards (PCI DSS) that may need to be addressed. While TokenEx can't complete your audit for you, we can help you to understand the process. Our team features several PCI Internal Security Assessors (PCI ISAs) that are experts on PCI DSS.

PCI Audit Timeline and Checklist

Throughout the Year (ongoing)

- ❑ PCI compliance is not just an annual effort. Continually review changes to systems, policies, and procedures to ensure your organization remains compliant between PCI audits.
- ❑ Identify evidence that is required, quarterly, bi-yearly, or annually, and gather as required.

Audit Opens (~ 1 month prior to onsite audit)

- ❑ Review the PCI DSS requirements, testing procedures, and corresponding guidance applicable to your organization.
- ❑ Document the compliance evidence required and assign an owner.
- ❑ Spend 2-3 weeks gathering compliance evidence. Make sure you have a date and version (if applicable) on all documentation, such as:.
    - ❑ Audit logs
    - ❑ Scan reports
    - ❑ Relevant policies

Final Preparation (~ 1 week before the audit)

- ❑ Identify key personnel that need to be available during the onsite audit.
- ❑ Gather final evidence needed for onsite audit. Aim to have 100% of the evidence available.

Onsite Audit

- ❑ Ensure that your key personnel have time blocked off to devote to the audit.
- ❑ Respond to questions from the auditors as they begin reviewing evidence.

Post Audit (4 to 6 weeks after the audit)

- ❑ Continue corresponding with auditors on follow-up questions. Be sure to inform them about any recent changes to your internal processes, controls, or key personnel.

Additional Tips

Consolidate audits. If you have other IT audits in addition to PCI (e.g., ISO, SOC 2), it can seem like your organization is in a perpetual audit. One solution is to conduct your audits at the same time. Since there are many overlapping requirements, you can reduce the time your team devotes to the audits.

Utilize audit management software. There are several systems (such as A-SCEND) that can significantly speed up the process of organizing and submitting information needed for an audit. You can also use the Prioritized Approach tool created by the PCI Security Standards Council.

How to Make the Audit Even Easier

The requirements in the PCI DSS are extensive because of the sensitive nature of cardholder data. However, TokenEx allows you to replace this sensitive data with a non-sensitive token. ***This can eliminate over 90% of the PCI DSS sub-requirements*** since TokenEx stores cardholder data, not your company.

You can simply rely on TokenEx's PCI Attestation of Compliance (AOC) to satisfy the PCI DSS requirements related to the storing, transmitting, and processing of cardholder data. See the table on the next page for additional details.

If you would like to learn more about how TokenEx can help you reduce your PCI DSS requirements, visit www.tokenex.com/pci

Preparing for Your PCI Audit: Tips and Checklist

PCI Audit Responsibilities

PCI DSS Category	PCI DSS Requirement	Number of Sub-requirements	
		Total	If using TokenEx
Build and Maintain a Secure Network and Systems	Requirement 1: Install and Maintain Network Security Controls	24	0
	Requirement 2: Apply Secure Configurations to All System Components	14	0
Protect Account Data	Requirement 3: Protect Stored Account Data	34	0
	Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	8	0
Maintain a Vulnerability Management Program	Requirement 5: Protect All Systems and Networks from Malicious Software	17	0
	Requirement 6: Develop and Maintain Secure Systems and Software	24	1*
Implement Strong Access Control Measures	Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know	15	0
	Requirement 8: Identify Users and Authenticate Access to System Components	32	7
	Requirement 9: Restrict Physical Access to Cardholder Data	32	5*
Regularly Monitor and Test Networks	Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	33	0
	Requirement 11: Test Security of Systems and Networks Regularly	24	1*
Maintain an Information Security Policy	Requirement 12: Support Information Security with Organizational Policies and Programs	40	1
	Total	297	15*

*Number of sub-requirements with TokenEx subject to change depending on assessment for PCI DSS 4.0 or PCI DSS 3.2.1.