PCI DSS Audit Timeline for Service Providers

Never have a false sense of security.™
**1 YEAR BEFORE**

Before you sign a contract, plan your path to compliance by determining what your specific needs are and what potential solutions can address them.

- First time PCI audit customers will:
  - Confirm your service provider level with the card brands
  - Engage with a Qualified Security Assessor (QSA) for an assessment
  - Confirm any scope reducing solutions you are using do not expire before your assessment

**9 MONTHS BEFORE**

- First time PCI audit customers will:
  - Start the initial gap process with a QSA
  - Review and make sure that your 3rd party providers’ attestation documentation and responsibility matrices are current
  - Confirm Approved Scanning Vendors (ASV) scans are happening quarterly on all appropriate targets and that discovered issues are remediated

**6 MONTHS BEFORE**

- Confirm that your policies/procedures are in place and updated
- Engage with the QSA company that will be performing your assessment
- Review the scope of the penetration test with your QSA
- Schedule your annual penetration test
6 MONTHS BEFORE (CONTINUED)

- If using segmentation, ensure your semi-annual segmentation test was completed
- Review your scoping exercise process and results with your QSA
- Discuss with your QSA any recent changes to your cardholder data environment (CDE)
- Establish a target date for you to submit your Attestation of Compliance (AOC)
- Set expectations for your timeline and schedule
- Discuss onsite/remote scheduling needs with your assessor

3 MONTHS BEFORE

- Create/Update network and card flow diagrams
- Schedule your onsite assessment
  - Determine personnel who need to be involved in the onsite assessment
  - Arrange for personnel to either attend or be available remotely
- Begin gathering and uploading evidence requested by your QSA to the assessment portal

1 MONTH BEFORE

- Finalize all travel arrangements for people involved in the onsite assessment

2 WEEKS BEFORE

- Obtain an agenda from your assessor
- Ensure all evidence requests in the assessment portal have been completed
- Verify all relevant parties are available for the onsite visit
1-30 DAYS AFTER ASSESSMENT

Remediation

*During this phase, you will work with your QSA to provide documentation to demonstrate compliance gaps identified during the assessment have been remediated.*

- Compliance gaps are documented in the assessment portal
- The QSA will discuss all assessment gap findings with the client
- The QSA will identify the type of documentation or follow-up reviews required to validate remediation work for each finding

30-45 DAYS AFTER ASSESSMENT

Draft Report Delivery

*The assessor will provide you with a draft version of your Report on Compliance (RoC) or validated Self-Assessment Questionnaire (SAQ).*

- Client and QA review of the draft report will be performed
- After all remediation work is verified, the audit lead will send the report and AOC for signatures
- The final report and signed AOC will be published to the assessment portal
An essential step of PCI compliance is an ongoing effort to maintain your environment and avoid situations that cause a higher compliance burden.

To ensure continued PCI compliance:

- **Maintain security policies**
  - Anytime you change the way you store, process, or transmit cardholder data, update your policies and diagrams to reflect the changes
  - Discuss significant changes with your QSA

- **Train your employees**
  - Inform new and current staff members how to correctly handle card data

- **Update your SAQ if things change**
  - Update and resubmit your SAQ if anything in your card processing environment changes

- **Run internal and external vulnerability scans**
  - Run scans at least quarterly
  - Run scans every time you make a network change

- **Verify you understand where your credit card data is stored**
  - Ensure all your credit card data is encrypted
  - Identify unencrypted card data with card discovery tools