CHECKLIST

securitymetrics®

PCI Assessment Preparation Timeline

Never have a false sense of security.™

CHECKLIST

Contents

Pre-Assessment

ONE YEAR BEFORE

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

- Establish your scope by addressing the following:
  - Engage with a Qualified Security Assessor (QSA) for an assessment
  - Confirm your merchant or service provider level with the card brands
- If you are renewing, confirm any scope reducing solutions you are using do not expire before your next assessment

9 MONTHS BEFORE

- First time PCI audit customers will:
  - Start the initial gap process with QSA
  - Review your 3rd party providers' attestation documentation and responsibility matrices
    - Check to see if they are current and accurate
  - If you are renewing, confirm Approved Scanning Vendor (ASV) scans are happening on all appropriate targets and that issues are remediated

6 MONTHS BEFORE

- Confirm that your policies/procedures are in place and updated
- When renewing:
  - Engage with the QSA company that will be performing your assessment
    - Ask your QSA any questions, particularly concerning tricky preparation steps you encounter
    - Go over the requirements you have
    - Establish a specific date for you to submit your Report on Compliance (ROC)
    - Set expectations for your timeline and schedule

NOTES

- Bring up any issues and discuss extensive changes with your auditor
- Review the scope of the penetration test with your QSA

Schedule your **penetration test**

First-time customers will:

- Begin **ASV scans**

3 MONTHS BEFORE

Obtain up-to-date network and card flow diagrams

Review evidence request list

Schedule your PCI Validation Assessment

Determine what internal personnel need to be involved in the assessment process

- Arrange for personnel to either attend or be available

1 MONTH BEFORE

Finalize all travel arrangements for people involved in the PCI Validation Assessment

TWO WEEKS BEFORE

Verify all relevant parties are available for the assessment

Double-check that visitors cannot access sensitive areas

- Consider your office plan for visitors

Ensure that managers/supervisors are informed of:

- Date assessor will be available
- What access assessor may need
- Any documentation required

Obtain an agenda from your assessor

Share the agenda with all involved parties

NOTES

PCI Validation Assessment

1-3 WEEKS ONSITE

The PCI Validation Assessment includes validation and documentation in order to produce a Report on Compliance (ROC).

- Project coordinator and audit lead will work together to identify dates to complete PCI DSS assessment
  - Sampling may be needed
- Go over steps to compliance with your QSA

Post Assessment

30 DAYS AFTER (REMEDIATION)

During this phase, your QSA works with you to determine what remediation needs to be done to ensure compliance.

- QSA identifies compliance gaps and puts them in the audit portal
  - Merchant works with QSA to understand finding and what evidence will be needed to close the finding
- Once remediation is finished, the merchant can upload the requested evidence to the audit portal for review

30-45 DAYS AFTER (REPORT DELIVERY)

You will receive a report on your audit describing the process and outcome.

- After all remediation work is finished, Audit Lead will release the completed SAQ D and AOC with the report

NOTES

ONGOING

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:

- Update **security policies**
  - Anytime you change the way you store, process or transmit cardholder data, update your policies to reflect the changes
  - Reach out to your QSA for assistance with your environment or changes
- **Train** 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 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**
- Verify you are properly monitoring and protecting your payment pages and have solutions to meet **PCI requirements 6.4.3 and 11.6.1**

NOTES

securitymetrics