PCI COMPLIANCE SOLUTIONS

Providing a High-Level Review of Your Company's PCI Obligations

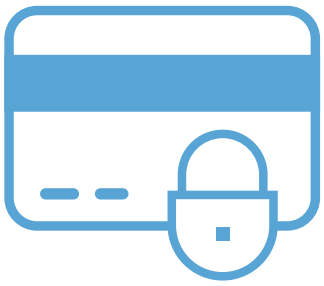
OVERVIEW

Any organization that stores, processes or transmits credit card data must comply with the Payment Card Industry Data Security Standard (PCI DSS). Optiv offers a wide range of PCI-related services that help your company achieve its compliance goals and build a sustainable compliance program regardless of where you are in the compliance cycle.

Optiv Payment Card Industry (PCI) Service Offerings:

1. PCI Executive Workshop
2. Readiness Review
3. Gap Analysis
4. Self-Assessment Questionnaire
5. Report on Compliance (RoC)
6. Payment Application (PA-DSS) Validation
7. QSA Remediation Guidance
8. PCI DSS Scope Reduction Strategy
9. PCI Penetration Testing
10. PCI Training

Receive customized consulting to create a plan for current and future compliance efforts.



Optiv's professional team is certified by all major credit card brands. We align organizations with multiple critical regulations.

Our Team

Years of Security Experience

Average Years of QSA Experience

MAINTAIN COMPLIANCE

Contact us for more details about PCI Compliance solutions.

888.732.9406

www.optiv.com

1. PCI Executive Workshop

Goal

To provide a high-level understanding of your company's PCI obligations.

Overview

These engagements typically focus on two of three areas: PCI awareness, cardholder data environment scope and key controls awareness/compliance. These areas of focus result in a high-level review and basic understanding of your PCI obligations. While we suggest that the Qualified Security Assessor (QSA) focus on education, scope or a specific item or issue, the QSA is available to support the client's PCI compliance needs for the engagement duration.

PCI REVIEW

- PCI Awareness
- Data Environment
- Compliance

ENGAGEMENT

- Determine Focus Interviews
- Documentation Review
- Review Payment Card Processing Methods
- PCI Education

TIME FRAME

- One to three days on-site

DELIVERABLES

- QSA Notes
- Presentation
- PCI Overview

2. Readiness Review

Goal

Review key controls through interviews to provide a high-level understanding of gaps in PCI compliance.

Overview

Typically combines on-site and remote interviews (teleconference) with key personnel, including business owners, network and systems engineers, developers, call center staff and security personnel. The on-site portion focuses on conducting interviews, performing walkthroughs of cardholder data processing environments and high-level documentation reviews.

ENGAGEMENT

- Information Gathering
- Interview Key Staff Members
- Review Pre-determined Documentation
- PCI Education

TIME FRAME

- Two to four weeks total
- Three to five days on-site
- 10-25 days remote assessments

DELIVERABLES

Key Controls Assessment Report

- Detail Each Key Control Assessed
- Detail Confirmed or Suspected Areas of Non-Compliance
- Provide Recommendations on Compliance & Remediation Strategies

3. Gap Analysis

Goal

Review all controls through interviews, documentation reviews and technical testing to provide a detailed understanding of gaps in PCI compliance. This understanding is critical when planning remediation projects, particularly for companies working on first-time compliance.

Overview

Focuses on all 12 areas of the PCI Data Security Standard and dives into the detail associated with each individual control. This analysis combines remote and on-site interviews, documentation reviews and walkthroughs of cardholder data processing environments, and examines process flows and all other areas associated with card-data processing and its associated and supporting systems.

ENGAGEMENT

- Review Policies & Procedures
- Interviews with Key Staff Members
- Review Data Card Systems
- Test PCI Controls

TIME FRAME

- Four to eight weeks total
- Minimum five days on-site
- 20 days remote assessment

DELIVERABLES

- Non-Technical Executive Summary
- PCI Environment Scope and Discovery
- Critical Findings Overview
- Findings and Recommendations

4. Self-Assessment Questionnaire

Guidance

Optiv can provide Self-Assessment Questionnaire (SAQ) guidance to companies that wish to sign their own SAQ. Optiv will base the level of effort on the number of days of assistance required; or,

Attestation

If Optiv will be attesting to (signing) the SAQ, then the following information describes the offering.

Goal

Conduct a PCI assessment consistent with an SAQ. The engagement will conclude in a completed Self-Assessment Questionnaire and Attestation of Compliance, which can be submitted to the credit card brands and the acquiring bank.

Overview

Focuses on all pertinent areas of the SAQ and dives into the detail associated with each required control. Assessment combines remote and on-site interviews with documentation reviews and walkthroughs of cardholder data processing environments, and examines process flows and all other areas associated with card-data processing and their associated and supporting systems.

ENGAGEMENT

- PCI Awareness
- Data Environment
- Compliance
- Test PCI controls, if attestation is required

TIME FRAME

- Determine Focus Interviews
- Documentation Review
- Review Payment Card Processing Methods
- PCI Education

DELIVERABLES

- QSA Notes
- Presentation
- PCI Overview

5. Report on Compliance (RoC)

Goal

Conduct a PCI assessment and review all controls through interviews, documentation reviews and technical testing. Engagement will conclude in a formal report on compliance (RoC), which can be submitted to the credit card brands and the acquiring bank.

Overview

Focuses on all 12 areas of the PCI Data Security Standard and dives into the detail associated with each individual control. Assessment combines remote and on-site interviews with documentation reviews and walkthroughs of cardholder data processing environments and examines process flows and all other areas associated with card-data processing and their associated and supporting systems.

ENGAGEMENT

- Review Policies & Procedures
- Interviews with Key Staff Members
- Review Data Card Systems
- Test PCI Controls

TIME FRAME

- Six to 20 weeks total
- Minimum five days on-site
- 20 days or more remote assessment

DELIVERABLES

- Non-Technical Executive Summary
  - Business Summary
  - Cardholder Data Environment Scope
  - Cardholder Data Flow Diagrams & Narratives
  - Network Segmentation & Wireless Environment Documentation
  - Summary of Systems Sampled & Persons Interviewed
  - Compensating Controls
  - Detailed PCI DSS Testing Results

6. Payment Application Validation (PA-DSS)

Goal

Conduct a PS-DSS validation of a commercially available payment application, with the end-goal of having the validated application listed on the PCI Security Standards website.

Overview

Focuses on all areas of the Payment Application Data Security Standard and dives into the detail associated with each individual control. The validation combines interviews with detailed documentation reviews of the implementation guide (IG) and examination of disk images to validate that cardholder data is protected per the PA-DSS.

ENGAGEMENT

- Review Implementation Guide
- Conduct Interviews with Key Staff Members
- Review Payment Application
- Test PCI Controls in a Lab Environment

TIME FRAME

- Six to 20 weeks
- Minimum five days on-site
- 30 Days or more remote assessment

DELIVERABLES

- Completed Report of Validation (ROV)
- Summary of Findings
- Scope Overview and Description
- Assessment Overview
- Findings and Observations
- Attestation of Validation (AOV)
- Submission of ROV, IG & AOV to the PCI SSC for Consideration
- Provide Recommendations on Compliance & Remediation Strategies

7. QSA Remediation Guidance

Goal

Partner as a trusted advisor to provide input on a PCI DSS remediation strategy and deliver on-guidance throughout the remediation effort.

Overview

Typically combines on-site and remote discussions via teleconference with key personnel, including business owners, network and systems engineers, developers, call center staff and security personnel to provide guidance from a PCI QSA perspective.

ENGAGEMENT

- Information Gathering
- Interview Key Staff Members
- PCI Education and Guidance

TIME FRAME

- One to 52 weeks

DELIVERABLES

- Discussion Notes
- Custom Documentation as Detailed in the Statement of Work

8. PCI Scope Reduction Strategy

Guidance

Provide recommendations on how to reduce an entity's PCI DSS scope in an effort to reduce recurring compliance costs and overall risk to cardholder data.

Overview

Evaluate current payment card process flows and business processes to determine potential options for P2PE/E2EE, tokenization and/or outsourcing of payment functions.

ENGAGEMENT

- Information Gathering
- Interview Key Staff Members
- Review Data Card Systems
- PCI Scope Education and Guidance

TIME FRAME

- Two to four weeks total to develop a strategy

DELIVERABLES

- Strategy Summary
- Current Card Processes Scope
- Recommended Solution Types by Type of Card Process
- Reduced Scope Potential

9. PCI Penetration Testing

Goal

To use industry best practices to conduct an internal and external penetration test to meet the requirements of the 11.3 controls within the PCI DSS.

Overview

Conduct network and application-layer penetration testing to validate that PCI controls and segmentation are in-place. Optiv also tests for vulnerabilities that could lead to the compromise of systems or sensitive data.

ENGAGEMENT

- Information Gathering
- Review Scope Documentation and Prior Tests
- Vulnerability Identification and Exploitation Attack Scenarios

TIME FRAME

- Two to four weeks total

DELIVERABLES

- Executive Summary
- Scope and Testing Methodology
- Vulnerabilities Identified
- Detailed Attack Scenario Narratives
- Segmentation Testing
- Recommendations

10. PCI Training

Goal

Provide training solutions that align with PCI DSS 3.1 training requirements.

Overview

Optiv's training services offer practical, real-world learning for employees and IT professionals. In addition to instructor-led technical training, we offer a number of PCI-specific eLearning courses that help clients meet the training component of the PCI DSS 3.1.

eLearning

Industry-recognized solution that helps organizations with their training requirements.

PCI-SPECIFIC COURSES

- Intro to PCI
- PCI Scoping
- PCI DSS
- Security Awareness for Credit Card Handlers

DELIVERY

- Fully Hosted Learning Management System (LMS) supported by Optiv
- Course Content Transferred to Clients' LMS
- On-Demand for Small Numbers of Users

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | optiv.com