



PCI Compliance Services

Reducing Cost and Risk



Challenges of PCI Compliance

Credit card breaches can be devastating, but securing credit card data is expensive and tedious. The Payment Card Industry Data Security Standard (PCI DSS) is long, technical, and periodically updated with new requirements and additional guidance. Many entities struggle to correctly identify the scope of their PCI environment, leading to compliance gaps. Other entities may not have a robust and well-documented PCI program, leading to confusion about who is responsible for which aspects of compliance. With the recent release of PCI DSS version 4.0, many have concerns about how to become compliant with this updated standard.

The Issue of Scope

PCI scope spreads through contact. Any system that touches the cardholder data environment is in scope. Many organizations believe that cardholder data must be stored in order to be in scope, but even transmitting card data creates PCI scope. Getting scoping wrong can lead to unpleasant surprises during a PCI assessment, but recognizing the true extent of PCI scope (and how much effort it will take to make every in-scope device compliant) can be daunting.

How Can KPMG Help?

KPMG LLP can help reduce the cost of compliance while simultaneously reducing the risk of breach. As a Qualified Security Assessor Company (QSAC) with seasoned Qualified Security Assessors (QSAs), KPMG has the skills and insights needed to improve your program. Our staff has years of experience in scope reduction, gap analysis and remediation, program building, acquirer communication, and more, to help our clients address concerns both before and after their PCI DSS assessment.

Scope Reduction

The best way to “win” at PCI DSS is not to play. KPMG can advise on scope reduction techniques to limit your cardholder data to the smallest possible footprint and reduce PCI program costs.

PCI 4.0 Readiness

Many entities that are currently attesting to PCI DSS version 3.2.1 are concerned about meeting the different requirements in version 4.0. KPMG can provide insight into new requirements and how to meet them.

Program Building

Whether an entity has a PCI compliance program that needs an uplift or no PCI compliance program at all, KPMG can help. Our QSAs can help with PCI policies and standards, PCI governance structure, PCI committee formation, and more.

Questions?

Contact our PCI Lead Partner, Adam Brand, to discuss how KPMG can help on your PCI compliance journey.

Adam Brand
Principal
Cyber Security Services
T: 312-282-9878
E: adambrand@kpmg.com

continued on next page >

Our Success Stories

KPMG has helped Fortune 500 companies and small organizations alike achieve their PCI compliance objectives.

Reduced Scope by 75%

While assessing the scope of a large international client, KPMG discovered that erroneous assumptions about PCI scope had been made, leading to the client's actual scope being much more expansive than the client initially thought. KPMG helped this client develop a plan to tremendously reduce scope.

Significantly Reduced Cost of Compliance

KPMG assisted a client with many subsidiaries, all of which had their own approach to PCI compliance. KPMG helped this client develop an organization-wide approach to PCI and introduce a formal PCI governance structure.

Navigated 65+ Changes

By analyzing a client's payment processes and reviewing their PCI DSS 3.2.1 approach to compliance, KPMG was able to note the applicable 4.0 changes and develop a plan to close the gaps before 4.0 becomes mandatory.

Keys to Delivery Success

KPMG prides itself on working closely and transparently with clients. We collaborate effectively by communicating our progress and concerns openly and frequently. We ask our clients to review deliverable drafts before finalization, so we can align on the right tone and focus for each unique audience. We also utilize technology effectively to accelerate work and avoid duplicate efforts. Let our experienced Qualified Security Assessor team work with you to help reduce your PCI compliance cost and risk.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



Additional Services

KPMG also offers additional PCI services, including:

- 1. Compensating Control and Exception Development**—Recommend compensating control and exception request strategies to address compliance in unusual circumstances.
- 2. Acquirer Communication Strategy and Support**—Develop a strategy for discussing extensions, fine reductions, and more with your acquiring banks and card brands.
- 3. PCI Initiative Management**—Assist with project management of major PCI transformation, evolution, or remediation projects, including subject matter know-how and executive reporting.
- 4. Selection Assistance**—Evaluate potential technology and service solutions to support PCI compliance and payment acceptance, such as payment processors and card readers.
- 5. PCI Solution Implementation Support**—Support throughout the design and implementation of new PCI-related processes and solutions, including developing requirement and architecture documents and reviewing implementations for compliance.
- 6. PCI Assessment Readiness**—Prepare detailed evidence collection playbooks, perform pretesting of controls, and assist with the development of an initial evidence package to provide the assessor.
- 7. PCI Assessment Support**—Provide project management support as well as helping field questions posed by the assessor.

Questions?

Contact our PCI Lead Partner, Adam Brand, to discuss how KPMG can help on your PCI compliance journey.



Adam Brand
Principal
Cyber Security Services
T: 312-282-9878
E: adambrand@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP412337