Payment Card Industry (PCI) Data Security Assessment Services

Is your company compliant with the Payment Card Industry Data Security Standard (PCI DSS)? Weaver is one of the few accounting firms to offer this level of certification as a Qualified Security Assessor (QSA) company registered with the PCI Security Standards Council.

Whether you're at the beginning stages of your PCI journey and struggling to figure out where to start, needing help to narrow down your scope, trying to understand PCI implications from a technology deployment, or looking for a PCI assessment, Weaver can help you navigate the journey. Our IT Advisory professionals bring a different level of service to our clients because of our roots as an audit firm. We approach payment card security from a business perspective, offering our clients a more holistic, risk-based service offering.

Why comply?

Compliance with PCI DSS brings benefits to businesses, no matter the size. Having a certified QSA assess compliance with the DSS can have many benefits for your organization:

▶ All merchants that accept credit card payments are required to comply with the DSS, even if they have outsourced payment processing. Engaging a QSA can help ensure your organization stays in accordance with the contracted terms of your acquirer.

▶ Third-party providers of certain services to merchants may need to assess their own compliance with DSS in order to provide those merchants assurance with regard to the outsourced services.

▶ Compliance with the DSS establishes a solid baseline for security practices as it relates to the cardholder data environment (CDE). The DSS aligns well with other security standards (e.g. ISO 27001, NIST CSF, CIS Controls, NIST SP 800-53) and can easily be extrapolated across the rest of your organization.

Overview of the PCI DSS goals and requirements:

▶ Build and maintain a secure network and systems using firewalls to protect cardholder data, and ensure that vendor-supplied defaults for system passwords and other security parameters are not used.

▶ Protect cardholder data and encrypt its transmission across open, public networks.

▶ Maintain a vulnerability management program with secure systems and applications, plus regular updates to anti-virus software and programs.

▶ Implement strong access control measures by restricting access to cardholder data (both electronic and physical) on a "need to know" basis.

▶ Regularly monitor and test networks and track all access to cardholder data.

▶ Maintain an information security policy that addresses information security for all personnel.

You can find more information on the PCI DSS goals and requirements at **www.pcisecuritystandards.org**.

weaver
Assurance · Tax · Advisory

Weaver's PCI DSS services include:

- ▶ Readiness and gap assessments
- ▶ Technology and scoping assistance
- ▶ Self-assessment questionnaire (SAQ) completion facilitation
- ▶ PCI DSS compliance assessments

For more information, contact:

Brittany George, CISA, CISM, QSA
Partner, IT Advisory Services
brittany.george@weaver.com | 972.448.9299

Brian Thomas, CISA, CISSP, QSA
National Practice Leader, Advisory Services
brian.thomas@weaver.com | 832.320.3280

We welcome you to visit Weaver's IT Advisory Services online at:
www.weaver.com/services/it-advisory-services.