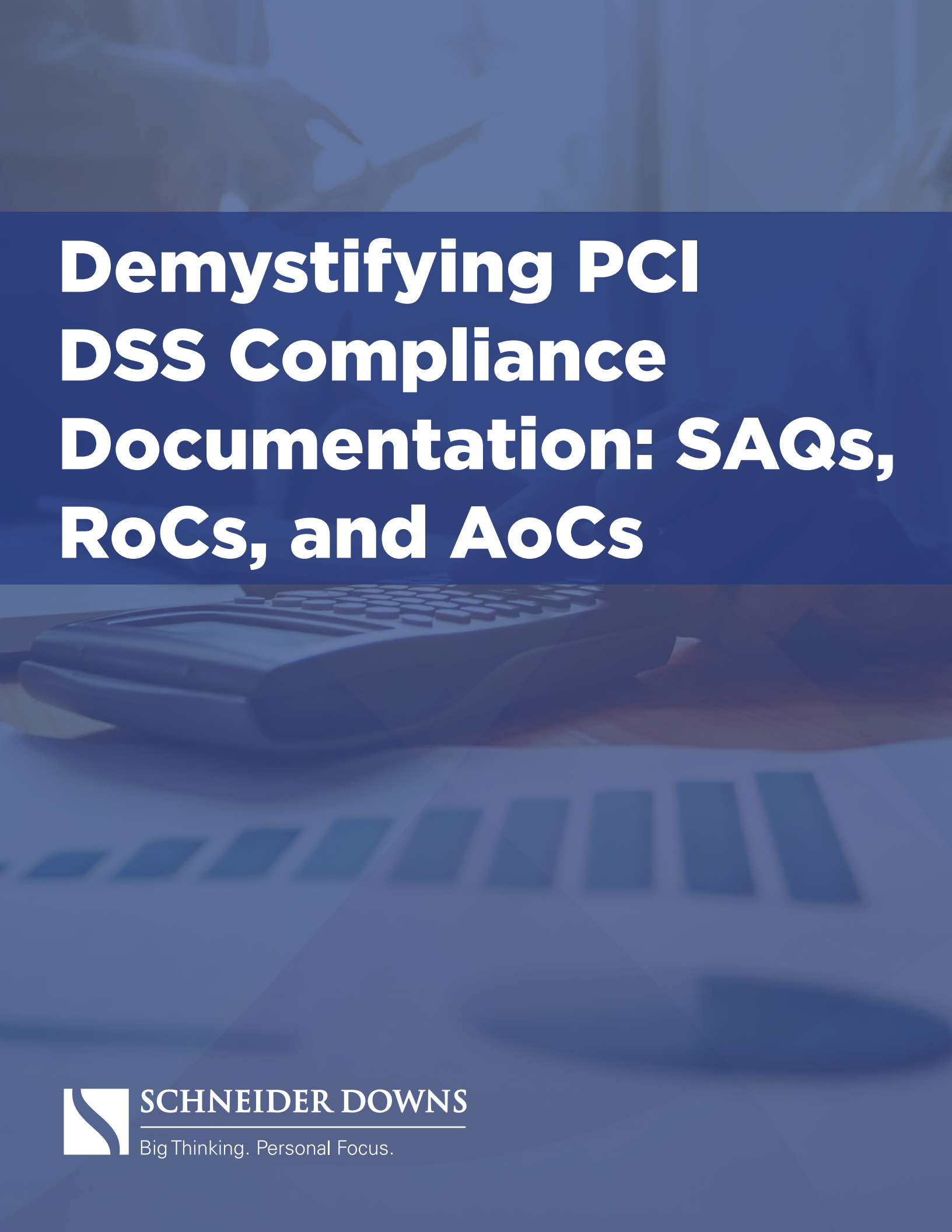

Demystifying PCI DSS Compliance Documentation: SAQs, RoCs, and AoCs

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Demystifying PCI DSS Compliance Documentation: SAQs, RoCs, and AoCs

For executives and financial decision-makers, navigating the complexities of the Payment Card Industry Data Security Standard (PCI DSS) often feels like parsing a foreign language. However, protecting cardholder data is not simply an IT issue; it is a fundamental business imperative tied directly to risk management, regulatory compliance, and bottom-line profitability. Organizations of all types—whether multinational corporations, mid-sized manufacturing firms, energy sector leaders, or not-for-profit entities—pursue PCI DSS compliance for critical reasons. These include meeting stringent regulatory requirements, establishing robust security postures, and securing legal protection as they process, store, or transmit credit card data.

Understanding the specific documentation required to validate your compliance is the first step toward reducing enterprise risk. The landscape of PCI DSS documentation primarily revolves around three core components: the Self-Assessment Questionnaire (SAQ), the Report on Compliance (RoC), and the Attestation of Compliance (AoC). Grasping what an Attestation of Compliance means, understanding the SAQ applicability to your specific transaction environment, and knowing when a Report on Compliance is mandatory will empower you to make informed, strategic decisions.

The Strategic Importance of PCI DSS Compliance

Before dissecting the specific reports and questionnaires, you must understand the strategic context. PCI DSS compliance is mandatory for any entity that handles cardholder data. Failing to maintain compliance exposes your organization to severe financial penalties, elevated transaction fees, and catastrophic reputational damage in the event of a data breach.

For the C-suite, managing this risk requires visibility into the compliance process. Acquirers (merchant banks) and payment brands demand verifiable proof that your security controls align with industry standards. You cannot simply state that your systems are secure; you must provide documented, meticulously gathered evidence. This is where the specific compliance documentation comes into play. By thoroughly understanding these reporting mechanisms, leaders can allocate the appropriate resources, avoid costly over-scoping of their cardholder data environment (CDE), and streamline the path to security validation.

The PCI Self-Assessment Questionnaire (SAQ): Meaning and Mechanics

A Self-Assessment Questionnaire (SAQ) is a critical validation tool used by a business that handles credit card data in any capacity to ensure it meets the necessary security requirements set forth by the PCI Security Standards Council (PCI SSC). The SAQ meaning extends beyond a simple form; it serves as a rigorous “checklist” of requirements detailing precisely how a business processes, stores, and transmits credit card data.

Completing an SAQ allows your organization to identify vulnerabilities and gaps in its security posture before malicious actors can exploit them. The assessment is typically performed by the business itself, utilizing internal security experts, or outsourced to a Qualified Security Assessor (QSA) company for objective, third-party validation.

Choosing the Right PCI DSS SAQ for Your Business Model

One of the most complex aspects of PCI compliance is determining which SAQ applies to your specific environment. Different SAQs have different requirements based entirely on how your organization utilizes credit card data. Selecting the incorrect SAQ can lead to false compliance declarations or force your team to implement unnecessary, costly security controls.

Here is a detailed breakdown of the various PCI self-assessment questionnaires:

- **SAQ A:** This applies to merchants that outsource cardholder data handling to PCI-DSS compliant third parties entirely. These entities have no processing, transmission, or storage of cardholder data on their own systems. This is common for businesses that use securely hosted iFrames for payment processing.
- **SAQ A-EP:** Designed for e-commerce merchants that maintain control over their website but outsource payment processing. An SAQ is still applicable to these entities because they remain responsible for the transaction security of the website itself, which could be compromised to redirect payment information.
- **SAQ B:** This questionnaire is for merchants that only have imprint machines and/or stand-alone dial-out terminals. Crucially, these merchants do not contain any electronic cardholder data storage.
- **SAQ B-IP:** This applies to merchants that do not store cardholder data on their systems but perform transaction processing via IP-connected POS terminals or terminals that are connected to the internet to transmit cardholder data.
- **SAQ C:** For merchants that have payment application systems connected to the internet but do not store electronic cardholder data. This often applies to small businesses utilizing specific point-of-sale software.
- **SAQ C-VT:** This questionnaire covers merchants that do not store cardholder data and manually enter it and process it via virtual terminals or web-based applications provided by a PCI-compliant third-party service provider. This is frequently seen in mail/telephone-order environments.
- **SAQ P2PE:** For merchants that use a strictly PCI-validated Point-to-Point Encryption (P2PE) solution. This advanced architecture allows the merchant to securely encrypt cardholder data at the point of entry and decrypt it at the secure endpoint, drastically reducing the compliance scope. As a best practice, confirm your P2PE devices are currently listed on the PCI SSC **website**.
- **SAQ D (Merchants):** This represents the most comprehensive assessment. It is for merchants that store, process, or transmit cardholder data and must be in compliance with the full suite of PCI DSS requirements.
- **SAQ D (Service Providers):** Designed specifically for service providers who store, process, or transmit cardholder data on behalf of clients, or who manage, support, or can affect the security of the cardholder data environment of another entity. These services require the service provider to adhere strictly to the full PCI SAQ requirements.

The Report on Compliance (RoC): Comprehensive Third-Party Validation

While many organizations can validate their security posture through an SAQ, higher transaction volumes dictate a more stringent approach. A Report on Compliance (RoC) is an in-depth, formal evaluation of a merchant's or service provider's adherence to the PCI DSS requirements. Unlike an SAQ, an organization cannot perform a RoC internally. It must be conducted by an independent, third-party Qualified Security Assessor (QSA).

During a RoC engagement, the QSA performs rigorous onsite assessments, interviews personnel, reviews system configurations, and analyzes network architecture. The resulting compliance report is a detailed document providing exhaustive evidence of the security controls in place.

Determining Your Merchant Level: Do You Need a RoC or an SAQ?

Whether your company requires a RoC or an SAQ depends primarily on your merchant level, which is dictated by the number of credit card transactions you process annually across all channels.

- **Level 1:** Organizations processing greater than 6 million transactions per year. These entities are mandated to undergo an annual RoC performed by a QSA.

- **Level 2:** Organizations processing between 1 million and 6 million transactions per year. These entities are typically permitted to complete an SAQ, though some acquirers may still request a RoC based on prior breach history.
- **Level 3:** Organizations processing between 20,000 and 1 million e-commerce transactions per year. An SAQ is required.
- **Level 4:** Organizations processing fewer than 20,000 e-commerce transactions per year, or up to 1 million total transactions. An SAQ is required.

Merchant Level	# of Transactions Per Year	SAQ or RoC?
Level 1	> 6 million	RoC
Level 2	1 million to 6 million	SAQ
Level 3	20,000 to 1 million	SAQ
Level 4	Less than 20,000	SAQ

By monitoring transaction volumes carefully, financial decision-makers can anticipate when their organization might cross the threshold from Level 2 to Level 1, requiring them to budget and plan for a transition from an SAQ to RoC.

The Attestation of Compliance (AoC): Your Final Declaration

Once the assessment process is complete—whether via an SAQ or a third-party RoC—the organization must formally declare its status. An Attestation of Compliance (AoC) verifies that an organization is compliant with PCI DSS requirements.

What is the AoC for PCI DSS in practical terms? It is the official, signed document that serves as your proof of compliance. An AoC is completed after the internal security expert or QSA has assessed the merchant for their compliance with PCI DSS standards. It is important to note that an AoC accompanies an SAQ or RoC regardless of whether the merchant performs the SAQ internally or outsources it to a third-party assessor.

Merchants typically provide the completed AoC to requesting entities, which include service providers, credit card companies, acquiring banks, or prospective business partners. For a C-suite executive, signing the AoC represents a formal acknowledgment that the organization has implemented the necessary security measures to protect cardholder data, carrying significant legal and operational weight.

Practical Steps to Achieve and Maintain Compliance

Approaching PCI DSS compliance requires strategic planning and disciplined execution. Leaders should establish a clear compliance program that operates continuously, rather than treating validation as an annual fire drill.

First, accurately define the scope of your cardholder data environment. Identify all systems, networks, and applications that store, process, or transmit account data, as well as any systems connected to them. Reducing this scope through network segmentation or technologies like P2PE directly reduces the cost and complexity of the audit.

Next, conduct a thorough gap analysis using the appropriate SAQ as your baseline. Identify missing security controls, outdated policies, or inadequate logging mechanisms. Assign clear remediation responsibilities to internal teams or external partners, ensuring that all identified vulnerabilities are addressed systematically.

Finally, gather and organize your evidence meticulously. Whether you are completing a self-assessment or preparing for a QSA audit, maintaining well-documented policies, configuration standards, and system logs will streamline the validation process and ensure you can confidently sign your Attestation of Compliance.

Partnering for Success: The Qualified Security Assessor Advantage

Managing PCI DSS compliance demands precision, technical acumen, and a strategic view of enterprise risk. As a Qualified Security Assessor (QSA) company, Schneider Downs pairs sophisticated expertise with a practical, human touch, helping leaders navigate these complex regulations and find new opportunities for business growth.

Our approach applies out-of-the-box thinking to your unique business model to reduce risk exposure, keep you compliant, and ensure your operations remain secure. We provide high-touch service through a responsive, collaborative team that is effective and considerate of your stakeholders' time. By partnering with a Trusted and Established Expert, you gain the clarity required to protect your data, satisfy your acquirers, and confidently attest to your security posture.

About Schneider Downs IT Risk Advisory

Schneider Downs' IT Risk Advisory professionals help organizations gain valuable insights into their processes and technologies. Our dedicated IT Risk Advisory professionals have experience working with a wide variety of industries and companies of all sizes. We will partner with you to provide comprehensive IT risk advisory reviews that will ensure your organization has effective and efficient technology controls that better align the technology function with your business and risk strategies.

For more information, please contact us at **contactsd@schneiderdowns.com** or visit **http://www.schneiderdowns.com/pcidss**.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003