VeriSign®

WHITE PAPER

Not All QSAs Are Created Equal:
What You Should Know Before You Buy

CONTENTS

The Payment Card Industry Data Security Standard (PCI DSS) requires Level 1 merchants and Levels 1 and 2 service providers to undergo an onsite assessment of their security systems and procedures annually. This assessment must be performed by a Qualified Security Assessor (QSA) as an employee of a Qualified Security Assessor Company (QSAC) and is designed to verify that an entity is complying with all requirements of the PCI DSS. Many companies, understandably, equate passing the assessment with actually being in compliance and having a strong security posture. However, recent security breaches highlight the danger of this assumption. True compliance and sound security are part of an ongoing commitment best serviced by QSAs with expertise in security as a whole.

This white paper helps companies choose the best QSA for their annual assessment by highlighting key differentiators among QSAs and QSA vendors (i.e., QSACs).

+ Misconceptions about PCI Compliance

Today's PCI Data Security Standard (PCI DSS) prevails as one of the most detailed models for strengthening security through compliance. The standards and associated testing procedures are rigorous. They address common weaknesses in information security practices and define a minimum level of security for account data. As part of business risk management, companies invest substantial time and effort in achieving and validating compliance with the standards. In doing so, they may believe that they have sufficiently protected account data; but validation of PCI compliance does not guarantee security.

The following myths about PCI compliance and validation can expose companies to significant risk:

- **Compliance = Security** – Complying with PCI standards isn't the same as having well-rounded security. A compliant company can still experience a security breach.
- **Compliance Today = Compliance Tomorrow** – Being compliant at a point in time (e.g., at the time of assessment) does not guarantee ongoing compliance. Companies—or independent business units within them—continually introduce, update, or change network components in order to support business growth. Change control is a complex process, and it is not always executed consistently. Lapses in security and compliance often occur because change management processes fail.
- **Compliance Validation = Compliance** – Being validated compliant by a QSA is not necessarily the same as being compliant. In one of the most serious credit card breaches this year, the merchant had been validated compliant; yet, a recent statement by the PCI Security Standards Council (SSC) reinforces its stance that the standard is a preventative against the type of breach that occurred. Up to 4.3 million unique accounts were stolen.

QSA CERTIFICATION REQUIREMENTS

The PCI requires validation assessments to be performed by Qualified Security Assessors (QSAs). These assessors must meet a number of business, administrative, and certification maintenance requirements, as well as possess basic qualifications. For example, QSAs must submit to background checks, have five or more years experience in the security field (or have a security certification), and pass a test. The test typically includes a mixture of multiple choice and short-answer questions. While QSA certification provides a baseline for evaluating QSAs, a company should always delve more deeply to identify the right QSA to meets its needs.

+ QSA Differentiators

As news headlines increasingly report security breaches and other events that suggest companies may be operating under misconceptions about compliance, prudent companies are choosing their QSA with more in mind than cost or passing a single assessment. Although all QSAs must meet the same set of requirements in order to become certified by the PCI SSC, QSAs vary not only in experience, aptitude, and thoroughness, but also in how they interpret requirements and the appropriateness of security measures and controls.

In selecting a QSA, companies should research potential vendors to ensure they can meet their unique needs and requirements. Companies can use the following indicators to help differentiate QSAs and QSA vendors:

- Staffing
- Auditing vs. assessment
- Project scoping
- Onsite follow-through and verification
- Feasibility of control recommendations
- Compensating controls
- Reputation and references

Questions for Your QSA Vendor

Ask the following questions prior to engaging a QSA vendor:

- How long has your company been in business and how many assessments have you done? What is the experience level of QSAs actually performing my assessment?
- What sizes and types of companies have you provided assessments for?
- Is PCI validation the only service you provide; what other security services do you offer?
- How would you staff the engagement?
- Is this quote for onsite assessment? How much of the assessment is performed remotely?
- I can provide answers to a lot of the questions about controls myself. How do you verify the accuracy of my responses and other documentation?
- What previous assessments or documentation do you use to gather data and evaluate compliance? How do you use them?
- What is your approach to implementing or identifying achievable controls? Can you provide examples of creatively meeting control objectives?
- Do you provide solutions for ongoing PCI program management, so that I can maintain compliance on my own?
- What is your stance on compensating controls?
- What sort of compensating controls have you put together?
- Which vendors do you partner with or recommend for compliance and security solutions?

RED FLAG – LEADING QUESTIONS

Pay attention to how the QSA asks questions. If the questions lead to an obvious answer or a yes/no response (e.g., "Your logs look like they are in order. Would you agree?"), the interview may yield an inaccurate picture of the company's security and compliance posture. Open-ended questions (e.g., "Tell me about your log review process.") usually elicit more informative responses and a more accurate assessment.

Staffing: The Two-QSA Minimum

Depending on the size and complexity of the environment, a proper PCI assessment requires a minimum of two QSAs, and as many as five or six, with experience assessing comparable systems. A properly performed assessment for a small to medium environment typically requires a minimum of two to four weeks to complete.

The assessment should always include a minimum of two QSAs to provide the following capabilities:

- **Technical skill set** – One or more QSAs should have expertise in assessing the technical components (e.g., mainframes, firewall logs, and databases) of the compliance/security solution.
- **Policy and governance skill set** – The other QSAs should have expertise in assessing whether policies and governance processes are sound and being followed.
- **Checks and balances** – No two people interpret PCI requirements, PCI assessment questions, and the security environment exactly the same. A QSA team can check one another for biases and assumptions.
- **Insight** – A QSA concerned with technical issues may ask different questions, focus on different answers, and arrive at different conclusions than a QSA focused on policies and governance. QSA team members complement each other during interviews to extract a more thorough and accurate picture of a company's security posture and compliance.

Auditing vs. Assessment

In evaluating QSAs, it helps to distinguish between auditing and assessment. Audits, by definition, determine whether a requirement is being met by looking at representative samples of a system. They typically rely on a checklist of yes/no questions and report results in terms such as pass/fail or compliant/non-compliant. The person performing an audit often does not have the background to delve more deeply into gray areas of security or compliance, or to recommend security improvements above compliance. In addition, the individual may not have the expertise to recognize and evaluate compensating controls.

Assessments take a holistic view of the security system, going further than a yes/no approach to understand how components and security measures work together to achieve compliance and maintain security. Assessors have more expertise in investigating and identifying holes in security, verifying security procedures and processes, and helping companies build on their existing resources to create a secure, compliant system. They use their expertise to not only assess the current state of compliance, but also to help ensure ongoing compliance and enable secure business growth.

RED FLAG – GLARING OVERSIGHTS

If the QSA overlooks areas that you know are non-compliant or poorly secured, check assumptions about the scope of the engagement. If the areas were in scope, the oversight may indicate incompetence and oversights in other areas.

RED FLAG – UNREALISTIC RECOMMENDATIONS

If the QSA recommends controls that do not make sense to you or require seemingly unreasonable changes or massive upgrades, seek a second opinion. Although a control may be achievable as recommended, a different solution may be less costly yet equally effective.

Project Scoping

The following factors help determine the size and complexity of an engagement. A QSA vendor should ask questions about these areas to help determine project scope and cost. If the vendor doesn't ask, it may indicate a lack of understanding about the assessment process, a lack of thoroughness, or a one-size-fits-all approach to assessment.

- Type of data stored (e.g., track data, account numbers, etc.)
- Volume of data stored; number of computers storing data
- Number and location of log files
- Data format
- Location of data (online or offline)
- Network segmentation
- Types and number of POS systems
- Types and number of third-party security services
- Number and location of external connections into the network

Onsite Follow-Through and Verification

A PCI assessment includes more than 240 unique control points and when performed properly, requires a significant investment of time. A thorough assessment entails more than asking questions offsite and accepting whatever answer the company provides. QSAs should verify that all answers are correct by spending sufficient time onsite to review and examine all settings, configurations, and documents on their own. For example, besides asking companies whether they have performed a quarterly log review, thorough QSAs would ask to see the logs.

Feasibility of Control Recommendations

No company passes a PCI assessment the first time. It is important to partner with a QSA that can provide an accurate picture of your overall compliance and security posture, recommend achievable controls, and work with you to create a solid strategy for ongoing compliance. Consider your current environment and constraints, and ask the QSA how he or she would address potential issues. Look for QSAs that are adept at finding creative solutions to meet requirements as well as using existing resources to build long-term solutions. Ask for examples of how they have done these things for other companies. The goal is to find a QSA that can recommend sensible solutions that optimize security and compliance while minimizing business impact.

Compensating Controls

The PCI DSS allows compensating controls when a company cannot meet the technical specifications of a requirement but has mitigated the relevant risk in some other way. Most companies must use at least one compensating control to meet PCI requirements. Frequently, this control is in the area of rendering card information unreadable (Requirement 3.4). However, as a matter of policy, some QSAs do not evaluate, accept, or suggest compensating controls.

RED FLAG – EASY PASSES AND LOW COST

If a QSA vendor charges much less than its competitors or has a reputation for easily passing companies, be cautious. It may not allocate sufficient time or staff to adequately investigate, validate, and consider all components and how they work together. Likewise, if an assessment was unexpectedly easy and you are surprised you passed, you may be risking non-compliance or a breach. Get a second opinion.

Compensating controls are not specified in the PCI standards, and they are often unique to each company. For this reason, PCI assessment of compensating controls involves more than basic auditing. It requires a deep understanding of security and the relationships between security components and systems. Not all QSAs have the expertise, creativity, and judgment to thoroughly vet compensating controls and determine whether they are acceptable.

Be sure your QSA endorses the use of compensating controls and has the breadth of experience needed to understand and identify them in a range of environments.

Reputation and References

As with any engagement, preliminary research about the QSA vendor may help identify strengths and weaknesses.

- **Use your network** – Ask your acquirer or business partners about the QSA vendor and about individual QSAs. They may not be able to provide outright recommendations (for liability reasons), but they may provide other useful information, such as how many assessments the vendor has performed compared to other vendors in the acquirer's network.
- **Check references** – Ask the QSA vendor for references from companies that are similar to yours and call them.
- **Consider the vendor's solutions and partners** – Solutions and partners should use open standards-based components that enable easy integration and interoperability with other components in your system, and do not lock you into a particular vendor.

+ Summary

Although all QSAs must meet a base set of requirements, they vary in skill, experience, and approach. These factors may impact the thoroughness and accuracy of the assessment you receive, as well as the QSA's ability to evaluate and improve your overall compliance and security posture. Before selecting a QSA and during the engagement, keep in mind the following considerations: staffing, auditing vs. assessment, project scoping, onsite verification, feasibility of control recommendations, compensating controls, and recommendations and references. Your QSA should have the breadth and depth of security and compliance expertise to function not merely as an auditor but as a partner who can provide in-depth assessment, recommend achievable controls, and help you develop a practical strategy for maintaining ongoing compliance and sound security.

+ VeriSign Global Consulting Services

Although many vendors offer services to companies seeking PCI compliance and assessment solutions, few providers match VeriSign's range of expertise, intelligence-gathering capabilities, commitment to open standards, or role as trusted advisor. VeriSign leverages regulatory knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and its history of stability and trust to deliver practical solutions that make the best use of existing in-house personnel, technology, and processes.

VeriSign's cost-effective, flexible portfolio of complementary intelligence, consulting, and managed services leverage the most current, real-world intelligence, experience, and technology to deliver proven compliance and protection solutions. As a trusted advisor, VeriSign supports customers through the evolution of a security initiative—vulnerability assessment, threat intelligence, technology reviews, and regulatory requirements—to define the best solution for the situation at hand and to build a long-term strategy for proactive security and compliance.

+ For More Information

For more information about PCI assessment, maintaining day-to-day compliance, or using existing assets to build a stronger security and compliance program, please contact VeriSign Global Security Consulting at 650-426-5310 or by email at enterprise_security@verisign.com.

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.VeriSign.com for more information.