All Qualified Security Assessors Are Not Created Equal

What You Should Know Before You Buy

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) requires Level 1 merchants and service providers to undergo an onsite assessment of their security systems and procedures annually. This assessment is typically performed by a Qualified Security Assessor[1] (QSA) and is designed to verify that an entity is complying with all requirements of the PCI DSS. Many companies assume that PCI compliance is synonymous with having a strong security posture, although recent security breaches highlight the danger of this assumption. Holistic, sound security practices are the building blocks for achieving PCI compliance, coupled with the astute use of the services of QSAs and security professionals who have expertise in network and data security.

This white paper provides some criteria to consider in choosing an appropriate QSA for your annual assessment by highlighting key differentiators among QSAs.

at&t

Misconceptions about PCI Compliance

Today's PCI DSS is one of the most prescriptive models for strengthening security through compliance. The PCI standard and its associated testing procedures are rigorous. They help unearth common weaknesses in information security practices and define a minimum level of security for protecting cardholder data. Companies invest substantial time and effort in achieving and validating compliance with the PCI standard. However, PCI compliance does not necessarily guarantee security of cardholder data.

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

Compliance = Security

Complying with PCI standards is not the same as having a robust security program. 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 system 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 can occur when change management processes fail, when changes are made without adequately considering the effect on security, and when security governance procedures are not followed.

Compliance Validation = Compliance

Being validated compliant by a QSA is not necessarily the same as being compliant. In three of the most serious recent credit card breaches, the compromised entity had been validated compliant by their QSA but was not truly secure. As a senior staff member of the PCI Council has stated about such problems: "what seems to be occurring is that organizations are going into this process with the mindset of passing a twice yearly physical." A "check-the-box" assessor may not be doing you any favors by stating that you are compliant when you really aren't, and not advising you on how to stay compliant going forward.

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 costs 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 how they evaluate the appropriateness of security measures and controls.

QSA Certification Requirements

The PCI DSS requires validation assessments to be performed by QSAs. In addition to meeting basic security qualifications, these assessors must meet a number of business, administrative, and certification maintenance requirements. 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 QSA exam. While QSA certification provides a baseline for evaluating QSAs, companies should always delve more deeply to identify the right QSA for their particular needs.

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

- QSA experience and staffing
- Audit versus assessment
- Assessment scoping
- Onsite follow-through and verification
- Feasibility of control recommendations
- Trusted advisor philosophy
- Compensating controls
- Reputation and references

Questions for Your QSA Vendor

- **How long has your company been in business?**
- **How many assessments have you performed? For what sizes/types of companies?**
- **What is the experience level of QSAs actually performing my assessment?**
- **What other security services do you offer?**
- **How would you staff the engagement?**
- **How much of the assessment is performed on site and how much 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?**
- **Do you provide solutions for ongoing PCI (and governance) program management, so that I can maintain compliance on my own?**
- **What is your stance on compensating controls? Can you provide examples?**
- **Which vendors do you recommend for compliance and security solutions?**

QSA Experience and Staffing: The Two-QSA Minimum

Depending on the size and complexity of the environment, a comprehensive PCI assessment requires a minimum of two QSAs, and up to as many as five or six for a complex assessment. An assessment for a small to medium environment typically requires two to four weeks to complete. The assessment should always be staffed by 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 configurations, and databases) of the compliance/security ecosystem.

Policy and governance skill set
QSAs should have expertise in assessing whether policies and governance processes are sound and being followed.

Experience and consistency
PCI assessments should be led by experienced QSAs who ensure that methodologies are followed in a consistent manner. In addition, the assessment team can check each other for biases and assumptions.

Insight
A QSA concerned with technical issues may ask different questions and arrive at different conclusions than a QSA focused on policies and governance. QSA team members should have complementary skill sets to extract a more thorough and accurate picture of a company's security posture and compliance.

Geographic proximity
Your QSA should strive to staff an engagement with at least one local QSA to encourage a relationship with a local resource and to reduce travel costs.

Audit Versus Assessment

Your QSA should take a "risk-based assessment" approach to the PCI compliance process. Clients may not be well served by QSAs who only take a narrow "audit" approach to compliance. Audits determine if a requirement is being met by reviewing representative samples of systems. They typically rely on a checklist of yes/no questions and report results in terms such as pass/fail or compliant/non-compliant. While AT&T does assess compliance on a point by point basis, an important strength of our approach is our willingness to delve into difficult or gray areas of security or compliance, and to recommend security improvements above technical compliance.

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 (i.e., "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.

Your PCI assessor should work closely with you to understand your business model and to take a holistic view of the security ecosystem, going further than a "yes/no" approach to understand how components and security measures work together to achieve compliance and maintain security. Good assessors should have strong expertise in investigating and identifying holes in security, verifying security procedures and processes, and helping companies build on their existing resources to improve security and maintain compliance. They use their expertise not only to assess the current state of compliance, but also to help ensure ongoing compliance and business growth.

Red Flag – Glaring Oversights

If the QSA overlooks areas that you know are non-compliant or poorly secured, try to determine the cause. If the areas were defined as in- scope, the oversight may indicate incompetence and raise concerns about overall adequacy of the evaluation.

Assessment Scoping

The following factors help determine the size and complexity of an engagement. A QSA should ask questions about these areas to help determine project scope and cost. If the QSA 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)
- Volume of data stored; number of devices 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. Beware of "fly-by" QSAs – a thorough assessment entails more than asking questions offsite or having companies send all of their evidence to the QSAs' portal and having the QSA accept whatever answer the company provides. QSAs should verify that all answers are correct by spending sufficient time onsite to review and examine 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 (during each annual assessment).

Feasibility of Control Recommendations

Perfect compliance is rarely a reality. It is important to work 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. It is critical for your QSA to understand your business and your cardholder data flows in order to perform a thorough assessment and make smart recommendations. Look for QSAs who are adept at finding creative solutions to meet requirements and to build long-term solutions. Ask

for examples of how they have done these things for other companies. Your QSA should be able to recommend sensible solutions that optimize security and compliance while minimizing business impact.

Red Flag – Unrealistic Recommendations

If the QSA recommends controls that do not make sense or are unreasonable (i.e., massive upgrades), seek a second opinion. Although a control may be achievable as recommended, a different solution may be less costly yet equally effective. Be wary of a QSA trying to "push" particular products or services.

Trusted Advisor Philosophy

Your QSA should be your trusted advisor regarding PCI strategy by working closely with you to help establish "compliance beyond the assessment". If any gaps are found during the course of your assessment, your QSA should not only point them out to you while on site, they should also collaborate with you to determine the remediation course of action and just as importantly work with you to determine the cause of the gap. In addition, your QSA should maintain strong communications with you throughout the year to inform you of any late-breaking developments in the PCI/security community and should be available as your Subject Matter Expert when discussing go-forward strategies.

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.

Specific compensating controls are not defined in the PCI standard, and they are often unique to each company. For this reason, compensating controls involve more than basic assessing. 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.

As a matter of policy, some QSAs do not consider the use of compensating controls. 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 business partners and your PCI network peers about the QSA vendor and about individual QSAs. They may not be able to provide outright recommendations (for liability or confidentiality reasons), but may provide useful guidance.

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. If an assessment was unexpectedly easy and you are surprised you passed, you may be risking your company's security and reputation and therefore you may want to get a second opinion.

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

QSAs should be product neutral, and willing to recommend the best solution for you, not just solutions from related companies.

Summary

Although all QSAs must meet a basic set of requirements, they vary in skill, experience, and approach. These factors may impact the thoroughness and accuracy of the assessment you receive. Before selecting a QSA and during the engagement, keep in mind the following considerations: QSA experience and staffing, audit versus assessment, assessment scoping, on-site follow through and verification, feasibility of control recommendations, trusted advisor philosophy, compensating controls, and reputation and references. Your QSA should have the breadth and depth of security and compliance expertise to function not merely as an auditor but as an advisor who can provide in-depth assessment, recommend achievable controls, and help you develop a practical strategy for maintaining ongoing compliance and sound security practices.

The AT&T Consulting Solution

Although many vendors offer services to companies seeking PCI compliance and assessment solutions, few providers match AT&T Consulting's range of expertise, intelligence gathering capabilities, commitment to open standards, or role as a trusted advisor. The AT&T Consulting solution 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 intelligent use of existing in-house personnel, technology, and processes.

The AT&T Consulting solution is a cost-effective, flexible portfolio of complementary intelligence, consulting, and managed services to deliver proven compliance and protection solutions. As a trusted advisor, AT&T supports customers through the evolution of a security initiative – vulnerability assessment, threat intelligence, technology reviews, and requirement assessment – to define the best solution for the situation at hand and to build a long-term strategy for proactive security and compliance.

The AT&T PCI Compliance Solution: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of PCI compliance and related security services. Our stability, experience and expertise, and commitment to open standards have established us as a strategic and Trusted Advisor for our customers. By leveraging AT&T you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your PCI compliance needs.

AT&T PCI-Related Services

AT&T offers several managed security services as well as additional security consulting services to help customers meet the requirements of the PCI Data Security Standard. These services include vulnerability scanning, penetration testing (network and application), incident response workshops, secure coding training, forensic review, and cardholder (or PII) data discovery. The AT&T suite of compliance and compliant services helps reduce the cost and complexity of meeting the PCI Data Security Standard.

For More Information

For more information about the AT&T PCI portfolio of services, maintaining day-to-day compliance, or using existing assets to build a stronger security and compliance program, please contact your AT&T Representative or visit www.att.com/consulting.

Note

1. The PCI DSS provides the option of performing a self assessment, but most large organizations use third party PCI compliance reviewers.

For more information contact an AT&T Representative or visit www.att.com/consulting.

06/16/10 AB-1918

at&t