Intro

PCI, unlike other regulations, standards, or certifications, has extremely cut and dry requirements for compliance. Simply, if your organization processes, transports, or stores credit cards in any fashion, you are required to comply with the Payment Card Industry standards. While this may be a necessity, there are tiers of compliance that are dictated by the total number of card numbers or payments accepted per brand card. Each brand card has a different total number of cards that will determine what level of processor or merchant your organization will be.

There is no shortage of vendors that claim to understand PCI. However, due to the nuanced nature of PCI, it is extremely important to select the right PCI security consultancies with whom to work. One of the first considerations when selecting a vendor is their expertise, and an easy way to determine that is to find a company that is a qualified security assessor (QSA).

The Best PCI DSS Consultants in the US

With a mature cybersecurity market in the US, it can be extremely difficult to find a quality vendor with whom to work. There are many vendors that are looking to cash in on a desperate organization, and it is often difficult to differentiate them from a highly experienced vendors. One way to determine a quality PCI vendor in the US market is to look for a QSA vendor and/or a VSA vendor. A company that has been reviewed by the PCI Council is likely to have a strong bench of consultants that can help guide your organization to compliance.

**Coalfire**

Coalfire is a highly recognized name in North America. This vendor brings a strong track record of technical, compliance, and strategic services to any engagement. Coupled with the fact that they are a QSA and VSA, this vendor will be able to help address an organization’s gap assessment, audits, or security program build. They may not be the cheapest vendor on this list, but they will not be the most expensive. With their flexibility, they can assist an organization in accomplishing its goals with a budget in mind.

**Optiv**

Optiv is known for providing a large selection of security services. An often-overlooked service is related to PCI. Like Coalfire, they are a QSA and provide services to help augment their QSA services. Optiv can provide gap assessments, program design and build, and certification. They have a large consultancy that allows them to have resources in many different regions within the US. Optiv may not conduct as many certifications as Coalfire or Viking Cloud, but they do provide many assessments and testing services for organizations looking to attain certification.

**Protiviti**

Protiviti is known as a strong technical consultancy firm. They are often overlooked for the services that they provide around PCI, which is a shame as they are one of the better options. They will provide a high-quality service to any organization looking to use them. With a strong technical understanding of PCI, any services utilized will be spot on and simplify the PCI certification process.

**RSM**

RSM provides many certification services beyond PCI. Being built on the back of CPA work, RSM will take a very methodical approach to their engagements. By bringing focused scoping and strong project management to the table, an organization will clearly understand what is being accomplished and why. Further, with their strong background across other security standards and certifications, RSM can assist with streamlining an organization’s compliance department by helping to identify common controls across these frameworks.

The Best International PCI DSS Consultants

PCI is not a North American certification; it is a brand label card requirement to process their cards. Because of this, any international or non-US-based organization will need to work with a vendor that can assist in their region. While many of the US-based consultancies can assist outside of the US, localization (language) may be a core requirement, so it is important to find a vendor that can assist in the language or location your organization operates in.

**BSI**

BSI is one of the largest security certification companies globally. With the ability to operate in the US and EU, BSI provides a large footprint to provide services. Much like RSM, BSI can assist with streamlining internal compliance requirements across multiple security standards or certifications. They also bring a strong technical skill set that allows them to dig deeper and wider to help strengthen a security program for PCI.

**PSC**

PSC may be the most internationally capable PCI consultancy on this list. Operating nearly across the globe, PSC brings an approach that works for large organizations, as well as small companies and startups. Known to dig deep and challenge their customers to go above and beyond the checkbox, PSC is a very strong partner to develop, implement, and improve the overall posture of the PCI security program for an organization.

**NCC Group**

The NCC Group brings a robust set of services that can assist any organization with continuity, response, cyber security, and even risk management. Due to this, NCC has become known as a strong solution provider for PCI services globally. They boast over 15,000 customers worldwide across their full portfolio. The NCC group brings a good mix of technical, project management, and compliance to any engagement to assist their clients in attaining and maintaining PCI certification.

Best Boutique PCI DSS Consultants

When it comes to PCI services, there are not many boutique shops that strictly or solely provide services in PCI. Many of the larger companies utilize PCI as a funnel, or way to increase their sales pipeline through lower-cost services. This makes it difficult for a smaller company to offer competitive services in this space. However, some companies do offer up services as part of their portfolio. When it comes to working with a boutique shop, it is recommended that you request to get the professional work experience of the main consultants that will be assisting you. If they are former QSA auditors for a larger firm, this will be an indication that they hold the expertise to assist your organization.

**403 Labs**

403 Labs’ main set of servers includes compliance audits, security assessments, penetration testing, and forensic investigations. While PCI may not be a daily core component of the organization, they have hired strong professionals with knowledge across multiple security frameworks and standards. This knowledge allows them to provide high-quality results, as their consultants bring an auditor’s view to the assessment and services.

**SecurityMetrics**

SecurityMetrics has built a suite of services that is focused on helping small organizations meet PCI requirements. This is something that is not easy for many small organizations, due to the number of controls and investment in tools and controls. Having a focus and expertise in small organizations has allowed them to develop an approach that has helped many companies meet PCI certification, regardless of the organization’s size. Couple this approach with their focus on other cybersecurity frameworks, and SecurityMetrics brings a strong understanding of running a compliance security program, regardless of standard.

The Best Value PCI DSS Consultants

Consider this a bonus category. The reality is that many of the vendors on this list provide affordable solutions for PCI. However, the two listed below have been known to provide quality solutions at a very affordable cost. When engaging vendors for quotes, always keep in mind that it is your organization’s responsibility to operate within PCI requirements. So, if you work with an extremely cheap vendor and have findings during an audit, those findings still need to be resolved. In short, practice caution when selecting an overly cheap vendor.

**VikingCloud** (Formerly SecureTrust, before that Trustwave)

VikingCloud has gone through several name changes and organization restructures recently. However, the core of their services related to compliance, including PCI, are still intact as part of VikingCloud. Those services have made the transition from Trustwave to SecureTrust to now VikingCloud. All of this being said, Trustwave has a strong brand reputation, and the expectation is that VikingCloud will retain that same recognition. Further, VikingCloud is considered to have the most QSA auditors in the world, as this is one of their areas of expertise. Due to having services that can cover the full spectrum of PCI, from program development to certification, VikingCloud is a solid option to discuss your organization’s needs.

**TrustNet**

TrustNet, like many of the vendors on this list, provides services across compliance and cybersecurity. Their ability to meet many of the major frameworks (PCI, SOC, ISO, HiTrust, etc.), shows that they have invested and continue to invest in security consultants that understand building and maintaining cybersecurity programs to meet compliance requirements. Further, they offer the usual services beyond compliance in penetration testing, risk management, and cybersecurity assessments. While they may not be massively cheaper than many of the vendors on this list, they will be affordable and provide quality results.

Tips on Choosing PCI DSS Consultants

Throughout this article, many points have already been mentioned about the difficulties and qualities that should be looked for in a PCI vendor. As stated previously, it is important to understand that PCI is a very prescriptive standard, which means that understanding and providing accurate recommendations can be difficult. The following tips can assist your organization in finding the right vendor for your requirements.

**Industry Experience**

Industry experience is extremely relevant when it comes to PCI. An organization that is in the retail space with multiple locations and point of sale systems is going to potentially be more complex than an eCommerce organization. Fully understanding the industry, along with how PCI will apply to that industry, will make the engagement more successful. When talking to vendors about your organization, it is recommended that you request references from other customers to ensure that there is sufficient experience in your industry. If this is not possible, at minimum, ask for case studies or other customers that the vendor has worked with.

**Partnership**

Entering conversations to find a partner in your PCI journey vs. a vendor is another way to maximize the relationship and improve the quality of work. This can be accomplished by discussing the full suite of services that the vendor offers and how those services can be paired together to help your organization streamline. Another reason to look for a vendor with a full lifecycle of offerings is that the PCI controls and requirements can often be complex, even for a smaller organization. By partnering with a vendor across multiple solutions, it provides the vendor the ability to better understand your organization and help provide more relevant recommendations that may save time and money.

**Technical Background/Knowledge**

This tip should not be confused with industry experience. When engaging a vendor, ask questions that will allow you to better understand the background of the consultants on staff or that the vendor will look to hire. As previously stated, PCI can be a complex standard to build controls for, and due to this, it is critical to have consultants that have the right technical background for your organization. A great example of this is related to network security controls. Implementation will be considerably different for an on-premises data center vs. a cloud-native deployment. While you can deploy virtual firewalls in your cloud infrastructure, there may be better ways to secure the network traffic and conduct the appropriate analysis that will save your organization time and money. Finding a vendor that has experience in your technology stack will allow them to better advise your organization.

**Project Management**

This last tip may be overlooked by many organizations, but it may be one of the biggest reasons for success or failure when working with a vendor. As part of the early conversations, discuss how the vendor runs their project management for their services. If the service engaged is a penetration test, it may not be overly relevant, but if it is a ROC assessment, it will be critical. Understanding how the vendor manages the hundreds of items, from request to review, will provide insight into the potential success of the engagement. Having a mature project management approach will assist in making the larger projects more successful and provide your organization with a higher quality product.