Best Security Compliance Companies

Intro

There is no lack of frameworks or regulations that any one organization will be required or voluntarily subscribe to. It used to be that if an organization is public, a set of regulations and frameworks were required. In fact, it doesn’t even matter if the organization is public or private, there are required and voluntary standards, regulations, or frameworks to be compliant with. To complicate matters, there are frameworks that are not security specific that have started to dip into security controls, which can make it extremely difficult for an organization to manage.

When it comes to compliance, an organization will need to first identify which regulations or frameworks will be required. Looking for a vendor or consultancy to assist with compliance will be futile until the requirements are identified. Requirements can be identified through government mandates, contractual clauses, or the type of industry the organization operates within. After this is completed and the required regulations and frameworks are identified, voluntary frameworks should be selected that may provide business value, reputation value, or that may help with maturing of the organization.

So, why would an organization look for a consultancy or vendor to help with meeting compliance? The short answer is that it can be complicated to manage controls, evidence, and documentation related to the framework. There are many ways to interpret a control or requirement in a regulation or framework. Not every environment is the same, so getting expert assistance when an organization is lacking internal skills is often the easiest way to blaze the path forward to a governance risk and compliance program (GRC) that can not only provide evidence of conformity on the first audit but provide a repeatable process.

The Best Security Compliance Companies in the US

It would be great if in these sections you could compare one to the other in any way, giving hints about what kind of client each company is best suited to.

When it comes to finding the right compliance consultancy or vendor, as previous stated, it is critical to have the regulations or framework identified. Some companies will excel at financial regulations, while having passable capabilities in other regulations or frameworks. Further, finding a company that has strong background in your organizations sector is also key, as this may assist with identifying more applicable regulations. For instance, a company in the financial services may identify PCI as relevant but when talking with a consultancy that works in the sector, the consultancy may find that PCI is not the right choice as the organization does not process any credit cards.

**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. Coalfire has been known to provide guidance and sit on several framework boards which provides it the ability to help guide the requirements for some of the common frameworks that are published. With their ability to assist across industries, and track record of working with some of the largest companies in the world, Coalfire is position to provide valuable services to your organization across almost any regulatory or compliance framework.

**Optiv**

Optiv is one of the largest security service providers in North America, and as such has worked with some of the most complex companies in the world. While it may not be known as well as their other services, Optiv has built a strong compliance consultancy service delivery team. Optiv is known for providing a large selection of security services. Optiv can provide gap assessments, program design and build, and certification. With their large consultancy, Optiv is positioned to have resources in many different regions within the US.

**Barr Advisory**

Barr provides services on par with Optiv and Coalfire, for both compliance and security. While they may not be as known as other larger firms, Barr has been providing strong services and advisory work for customers across HITRUST, SOC2, ISO27001 and FEDRamp over the years. Along with their internal capabilities, Barr has built out a global network of partners to assist clients with their compliance requirements regardless of location.

The Best International Security Compliance Companies

**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. With being one of the largest certification organizations in the world, this comes with a need to provide consultancy services. This positions BSI to leverage highly experienced auditors to validate the consultancy practice. Further, they have built a separation between their certification and consultancy business which would allow your organization to leverage them for both the build and certification of your security program.

**KPMG**

KPMG is a highly recognized brand that may not be known for the services that they offer outside of their CPA offerings. However, they have a very large certification, audit, and security services arm that is very strong across the board. With this large division, KPMG has become a very strong provider of advisory services and offerings to assist clients with meeting compliance requirements. With their strong international presence, work with large enterprise, KPMG has developed a mature compliance advisory service.

Best Boutique Security Compliance Companies

**SideChannel**

SideChannel offers many services beyond compliance and is best known for their vCISO services to small to mid-market companies. They are especially adept at working with startups, which makes them equally capable of assisting with many of the compliance requirements a company would have. The ability to build a security program, with their extremely experienced group of ex-CISOs, provides a lot of industry knowledge and hands on experience that is hard to find in many companies.

**Risk3Sixty**

Risk3Sixy is a rising boutique shop that has put forward a lot of time and effort into building internal and external tools to assist with compliance. Like many on this list, they offer services for the core frameworks and regulations that most companies will encounter. But to add additional value, they have built a full GRC platform that their internal team utilizes for many of their engagements. So, if your organization were to use Risk3Sixty, there would be value in considering their GRC tool as it may streamline the ability for their consultants to help manage your compliance requirements.

The Best SaaS Security Compliance Companies

**Drata**

Drata is a pure play compliance SaaS solution. Drata does not really provide consultancy services but does offer professional service assist with setting up their solution. While the product is still fairly new, it has gained recognition for the ability to ease the burdens of attain certification against the provided frameworks. Drata is still working on building out capabilities to assist with managing frameworks, and to date has focused on PCI, ISO27001, NIST and SOC2, but it is planning to continue to add additional frameworks. When evaluating solutions, it is worth reviewing Drata as they provide an automated way, for many of the controls, to gather evidence and manage compliance with the requirements of the frameworks.

**Vanta**

Vanta is very similar to Drata. They offer a SaaS solution that allows for the automated gathering and auditing of controls across an organizations IT environment. Further, they have a long list of partners for both internal and certification audits to streamline the audit process as the approved auditors are able to utilize their platform to review your evidence, documents, policies, and other supporting material. Just like Drata, Vanta does not offer consultancy services but they do offer professional services to assist with onboarding to their platform. With their platform built to manage your security program, onboarding and loading evidence assists with showing compliance with the framework.

Tips on Choosing Security Compliance Companies

Give 3-5 tips on choosing one of these companies: How can you know which one will be best for your firm, other than by price?

When it comes to selecting the right consultancy for your compliance project, the following tips can help your organization in finding the right partner and managing cost.

**Expertise**

This may seem obvious but plenty of organizations have fallen prey to an assumption that compliance is compliance regardless of the framework. This simply is not true and could cost your organization time and money to rework your program if you pick the wrong partner for your project. FEDRAMP is significantly different, and more intensive, then ISO27001. Finding a partner that has the expertise in your framework or regulation is key. Spend the time to understand which framework or regulation you need to meet and interviewing your potential partner to understand their experience and previous projects.

**References**

When it comes to finding a good partner, beyond the name brands or highly marketed vendors, it can be difficult. In this case, reach out to peers in your industry or city and ask for references for partners to assist with your compliance projects. This service is very common and many organizations leverage third parties to assist with their compliance obligations. When talking to your peer, ask what they liked, did not like and what they would do differently.

**Environment**

Not every environment is the same, not every organization operates the same. So, when interviewing your potential partners, use specifics with them about your environment. See how they respond, do they include specific examples that are from similar environments or architectures as yours? If not, directly ask how they manage or assist a company with building their program with your specific environment requirements. Building a compliant security program for an AWS native application is different than building for an VM based application. There are different tools and services that can be leveraged for both, often time saving time and effort for your team.