WHITE PAPER

blue umbrella

Key factors in choosing a third-party compliance platform

Published by Blue Umbrella

Contents

Overview

Third parties represent one of the largest compliance risks to any organization. Designing and assembling a third-party compliance program is a challenge in and of itself. As multinationals grow in scale, increase their international scope and utilize more high-risk vendors, agents, distributors and channel partners, crafting a program to comply with the Foreign Corrupt Practices Act (FCPA), the UK Bribery Act (UKBA) and other ABAC regulations to becomes an ever more daunting task, as does guarding your reputation and regulatory risk.

However, the real challenge in third-party compliance is not program design but program operationalization. Countless programs have moderately well-documented third-party compliance strategies, but when it comes to operationalization, they are disorganized, imbalanced in their application and ill-equipped to identify risks, trends and remediation. These programs' inability to operate is an obvious shortcoming that can only really be addressed, especially in large companies, through the effective roll-out of technology.

There is a plethora of technology options in third-party compliance, from internally programmed systems, which often use a foundational program like SharePoint, to purpose-built technologies provided by vendors. The strengths and weaknesses of each of these technologies varies hugely. Finding the right technology to fit all aspects of your program, your department and your geographic footprint is a challenge.

This whitepaper is meant to guide you through several key areas to consider when evaluating what technology is best for your company.

1.Macro-level Concerns

One of the most important elements to consider when choosing a technology is the assessment of several nuanced, macro-level characteristics of the technology and potential provider.

1.1 Vendor Background

Assessing the very core of the company that is providing compliance technology is critical and should be cross-referenced with the most important parts of your workflow. Vendors can be classified into several categories: database providers, due diligence report providers, technology providers, or various combinations of these. The skills involved in each of these different elements vary greatly so choosing a company that matches your needs is important.

If you have high-risk relationships globally, finding a company that provides high quality due diligence will likely be integral to your success. For example, if you have chosen a pure technology vendor and you have questions for the vendor regarding your due diligence reports, consider how answers to your due diligence questions will migrate back to your team.

On the other hand, if you have many very low-risk relationships and will be using databases as the primary risk management tool, perhaps a vendor that is strictly a database provider will prove to be most beneficial in the future.

Alternatively, if a company is strictly a due diligence provider that has its own operations but does not fully understand technology and outsourced that to a third-party operation, it will increase challenges with implementation and limit ongoing technology development. It is crucial for any provider to have an in-house programming capability.

KEY QUESTIONS TO CONSIDER

- ☐ What kinds of services does the vendor offer (i.e. pure technology provider)? Do they meet your compliance needs?
- ☐ How will the vendor deliver services that are not kept in-house? How will the vendor answer exceptions or issues with those outsourced services?
- ☐ What is the company's global footprint?
- ☐ Does the vendor have in-house programming capabilities? Who will be doing the programming? How big is the team? Can you meet the IT Director?

On both an ideological and practical level, a vendor's presentation and the way they conduct themselves is also important. The personalities of the people you will conduct business with are crucial to forging positive and mutually beneficial long-term relationships. Meet with the senior executives and understand the company's values, ethics and approach to working together. If you cannot access senior managers, note this as a possible red flag that could arise again if you have serious implementation issues or other issues. Third-party compliance programs are not

easy to manage. They require work, attention to detail, dynamic management and collaboration to adapt to changing environments. If your character and the character of your business matches well with the vendor, it will ultimately prove to be extremely beneficial.

One of the easiest ways to assess whether the background of the firms you are considering is a good fit is to not only meet and interact with senior executives, but also to contact references. Every company should be able to provide several good references. Request references for different situations and ask questions like the following to assess the breadth of the vendor's resources and client management system:

- ☐ Provide a reference for a client that had some challenges with onboarding to your system.
- ☐ Provide a reference that has recently undergone your onboarding process.
- ☐ Provide a reference that can attest to your ongoing account management program.

Assessing a vendor's references based on key areas of concern is more effective than requesting several references and asking them basic questions without a directed purpose.

Ownership background should also be carefully examined. Investigate who owns the company and their motives. If the company is owned by private equity, understand that the company is very likely to change ownership within the next three to five years at maximum, and that the company values and business dynamic will likely change with it.

KEY QUESTIONS TO CONSIDER

- ☐ Have you asked for references that are tailored to specific situations, not just a general call for references?
- ☐ What are the vendor's company values?
- ☐ Do the vendor's client referrals provide positive feedback about the company's capabilities?
- ☐ Is the vendor owned by a private equity or is it privately owned?
- ☐ What is the vendor's strategy for market expansion? How will the vendor's strategy curtail with your own compliance program goals?

1.2 Digital Debt

Digital debt is a concept that is not unlike financial debt. At its base is the understanding that any technology begins to age as soon as it is built, and the decisions made about a technology's architecture, physical and digital, can preclude its flexibility or continued innovation.

How does this manifest itself in third-party compliance? Companies with an excess of digital debt are platforms built upon unsuitable, rigid foundations. They will have trouble with adding functionality, adapting to changes in your program and including new technologies as time progresses. For instance, if a vendor technology was originally designed on an older technology or for a different industry purpose, it is likely ill-suited for your company. If the technology was not purpose-built for your personal needs, it will be a poor match.

In order to assess digital debt, it is important to understand an organization's effectiveness with paying its digital debt. This assessment can be accomplished by evaluating 3 categories:

1. **System foundations:** Investigate the foundations of the system and whether the system was originally designed for the purpose of third-party compliance.
2. **Client specificity**: Examine the application and its database to evaluate whether consideration was given to client-specific elements. Consider whether the fields, workflows and structures are configurable to your own organization's terminology, flows and requirements.
3. **Wholesale upgrades**: Investigate the date of the latest wholesale upgrade to an application, database or other structural element of the technology.

Many organizations are recalcitrant about paying digital debt. Paying this debt requires planning, resources and forethought. If there has been no consideration toward this, even if the technology suits your organization well now, challenges will almost certainly develop over time.

KEY QUESTIONS TO CONSIDER

- ☐ What are the foundations of the system? Was it originally designed for third-party compliance?
- ☐ When designing the application and its database, was consideration given to which elements are client-specific?
- ☐ How many fields, workflows and structures are client-specific? What are they?
- ☐ What is the date of the latest wholesale upgrade that was made to an application, database or other structural element of the technology?
- ☐ Has the vendor clearly demonstrated that they are actively combatting digital debt?

1.3 Flexibility

The assessment of technological flexibility is also relevant to discussions concerning digital debt. No two compliance departments are the same. Each has their own terminology, structure, workflows and risk appetites. The job of a technology provider is not to convince you to change your processes to suit their technology, but rather to meld their technology around your processes. If a technology is too rigid and forces you to create operational workarounds, it can generate large gaps in your processes and essentially take them offline.

The best way to assess flexibility prior to choosing a vendor is to engage the provider in thorough conversations and live demos, which will demonstrate how the system will conform to your precise environment and workflow. By outlining the framework of your specific department and its processes, and by asking the vendor to accommodate for it in their system, you can consolidate a sufficient amount of detail to assess what may be possible within the system and where possible frustrations may occur.

It should be noted that benchmarking and advice should not be mistaken for technology rigidity. Your compliance workflow exists as it does for good reason. Although benchmarking is

valuable, if the key desire of a provider is to compress your processes into a workflow or process that exists in their system rather than working around your needs, it can be entirely counterproductive.

KEY QUESTIONS TO CONSIDER

- ☐ What third-party compliance workflows are available within the proposed platform? Are they limited?
- ☐ What is the maximum number of workflows? Will this number enable or restrict your processes?
- ☐ How can the platform adapt to your workflows and processes?
- ☐ Does the platform allow you to modify a pending workflow?

1.4 Hierarchy

Every compliance department differs geographically, hierarchically, and in the manner that it gathers and communicates information to and from other business units. Whether your organization is extremely centralized, with all third-party compliance passing through one central global team, or if it works through a more federated model, the system should possess the capability to provide different rights to different users.

Even if your current program is relatively small and does not require functions to limit access or to restrict viewing rights by user, your program will almost certainly adapt and grow over time. The ability to limit access for users in the future may become increasingly important as your program expands. Consider a scenario where you may be required to rely on some short-term assistance for a remediation project. It may be prudent to give them access to only the information they need and limit their ability to incur expenses through ordering.

KEY QUESTIONS TO CONSIDER

- ☐ What levels of authority can be assigned within the platform?
- ☐ Can the platform restrict actions such as ordering due diligence or accessible information by user authority?
- ☐ Can the administrator contact other users (i.e. post news on the main page, email different categories of users)?
- ☐ Can the administrator send group emails to third parties?
- ☐ Are there tools to record user logs and important user activity?

1.5 Automation and Efficiency

Technology systems exist to simplify our lives and relieve unneeded burdens, not to engender frustration and needless complications. With the era of automation upon us, and with the requirements of our programs to manage ever greater numbers through increasingly complicated workflows, it is crucial for technology to assist us with repetitive, administrative burdens. This way, experienced compliance personnel can concentrate on high level tasks such as program design, issue handling, remediation, decision-making and trend spotting.

There are possible pitfalls to automation. For instance, automation can be far too prescriptive. Rather than seeking a vendor that can automate several different workflows, seek a vendor that has a robust “rules wizard” automation engine. With a “rules wizard” automation engine, any automation can be accomplished as long as there is a defined criterion and an outcome. This method ensures you will not be limited by a vendor’s proposed automations and that you can incorporate any automation, no matter how large or small, into your customized workflow.

Look for other efficiency tools that will support your needs. Nobody understands your program as well as you and your team do. Identify the pain points in your workflow, where there is far too much administration for too little return. If, for instance, you find an unnecessary amount of time is spent working with your business leaders to commence the onboarding process for a new third-party, ensure the technology can deal directly with requests originating from the business. Likewise, if the majority of your work deals with your third-party questionnaire, ensure the questionnaire function of your chosen platform is sufficiently robust to eliminate large amounts of that work.

KEY QUESTIONS TO CONSIDER

- ☐ Does the platform have a robust “rules wizard” to incorporate any automation?
- ☐ What reminders, renewals and recertification’s can be set within the platform?
- ☐ What other third-party compliance automations are available within the platform?
- ☐ What automations are available related to due diligence?
- ☐ What other efficiency tools are available to use?

1.6 Integration

Compliance departments do not exist in isolation and neither should technology. An excellent technology system should allow for integration with other technologies such as your customer relationship management (CRM), finance, procurement and internal systems. Investigate integrations that the vendor previously completed and request references from other clients who have worked on integration projects.

KEY QUESTIONS TO CONSIDER

- ☐ Does the platform integrate with other systems? If so, which ones?
- ☐ Can the company migrate information from an existing database to the platform?

1.7 Technology Leadership

Technology is developing at a breakneck speed. Automation, deep learning, natural language processing and big data will all completely disrupt the way traditional third-party compliance is conducted in the next few years. Choosing a vendor that has shown leadership and the desire to be disruptive will help you avoid technologies that will become redundant, ensuring you will not be forced to change vendors in one or two years. Assess their understanding of these future technologies and how they will reshape their compliance function in upcoming years.

KEY QUESTIONS TO CONSIDER

- ☐ Is the company disruptive?
- ☐ How is the company demonstrating technology leadership?
- ☐ Does the company demonstrate awareness of future changes to technology and compliance?

2.User Experience

Many business software lacks user-friendliness. With a strict focus on technical detail, the majority of software providers overlook the importance of platforms to appear and function in a way that is simple and pleasing to its users.

Furthermore, the breadth of many systems is worthy of discussion. Some systems provide not only third-party compliance but also whistleblower services, training modules, policy management, case management and more. While it may be tempting to invest in all of these functionalities at once, consider not only your need for these additional modules, but also what will be achieved by having them all in one platform. For instance, although policy management is important, you should consider whether or not it is beneficial for your team to use a policy management system from the same provider of your third-party compliance system. The synergies created by using multiple modules from one provider are few and far between and, overall, will have a limited positive impact on your program.

Assessing user experience is not always easy. Demonstrations are paramount in this regard and should be a mainstay of any purchasing procedure. Typically, for a more major roll-out, 3-5 demonstrations are required in order to establish a good understanding of how a particular system operates and what issues may arise from its configuration. Ask potential vendors to run through your workflow on their system so you can understand the system's functionalities.

Another key to user experience is the offline availability of the vendor. If you have a global organization, will there be regional contacts with which you can discuss technology or research?

KEY QUESTIONS TO CONSIDER

- ☐ Is the platform easy to navigate and user-friendly?
- ☐ What third-party information can be collected in the platform?
- ☐ What are the maximum number of sign-ins or number of users?
- ☐ What metrics does the platform provide, in what format and for which users?
- ☐ Can the third-party provide data online?
- ☐ Can the platform consolidate certifications per business line?
- ☐ What file formats are available for the export of information?
- ☐ Are bulk uploads available?

3.Integration of Content

The purpose of a third-party compliance program is not just to implement a set of controls through technology. It is to demonstrate that you have made an effort to understand the third-party's identity. Therefore, content provision through the platform is extremely important.

If you have a global organization, assess whether the vendor has the research resources available to meet this demand. A vendor that holds a very close relationship with their research is likely one that is more capable of integrating their research into the platform.

KEY QUESTIONS TO CONSIDER

Due Diligence

- ☐ Does the vendor have sufficient research resources to meet your demands?
- ☐ Can various types of information be cross-referenced and compared within the platform?
- ☐ What levels of due diligence are available? What do they encompass?
- ☐ Is the due diligence performed in English and local language of the subject?
- ☐ Does due diligence collected on a third-party integrate within the platform and affect the risk rating of a third-party?

Vendors that are closely tied to their research are ones that conduct research in-house and train their research analyst employees by a standard procedure to ensure quality control. Consistency of methodology is important in maintaining an effective system of controls. If a vendor's due diligence services are provided for by a partner or a network of subcontractors or freelancers instead of in-house researchers, the information in the reports is likely delivered through a strict document upload. Risks observed in the report, related entities, the ability to cross-reference questionnaire answers with the due diligence and other vital information will not be integrated into the platform for your easy review. There may also be security issues with research conducted by subcontractors, freelancers or independent contractors operating on personal computers or unsecure networks.

KEY QUESTIONS TO CONSIDER

Research

- ☐ Is the research performed in house by full time employees or by subcontractors (defined as outside companies, independent freelancers, or part time employees)?
- ☐ How is quality control maintained for research? How are the researchers trained?
- ☐ How many researchers does the vendor employ and where are they located?
- ☐ Are there security concerns with researchers operating on personal computers or unsecure networks?

KEY QUESTIONS TO CONSIDER

Database Screening

- ☐ What is the vendor's database screening capability and what datasets are included in the offer?
- ☐ What are the available cadences of your screening (i.e. continuous, monthly, quarterly)?
- ☐ What measures are taken to remove noise, such as false positives, from the screening process?
- ☐ Does the vendor offer managed screening to eliminate false positives? If so, who performs this analysis?

4.Pricing

There are a multitude of different pricing models on the market. As more private equity money moves into the industry, most vendors are rallying around one model: require multi-year agreements, charge annual licensing fees, maintenance fees, integration fees and other technology-related fees to maximize the Annual Re-occurring Revenue (ARR) and price-to-earnings (P/E ratio) of a company for an exit strategy. Note that this strategy does not account for the desires of the customers, but exists strictly to maximize a specific line item in order to increase the apparent value of the firm for a sale.

Note also that these firms also charge for content on the platform. Rather than paying for both the content and the right to use the technology, find a provider that allows for platform access and use without annual fees or hidden technology fees.

A natural corollary of working with a vendor that charges annual fees is that there will be a guaranteed, multi-year contract. As discussed, technology is disrupting the entire industry and there is no guarantee that the technology that you pick today will still be the most suitable in two or three years. It is always more advantageous to avoid an annual licensing arrangement as you will not be bound by a contract.

Understanding and documenting additional fees is also helpful. For instance, if changes need to be made to the system, it is valuable to understand how they will be configured into the system, the expected turnaround time of the requests and what extra fees might apply. Also consider the medium- and long-term requirements of your chosen compliance system, which may include integrations with other systems, increasing the size of your third-party universe or increasing the number of users.

KEY QUESTIONS TO CONSIDER

- ☐ Are there annual, licensing, subscription, or per seat fees?
- ☐ What are the fees associated with implementation?
- ☐ Is there a cost for setting up Single Sign On (SSO)?
- ☐ What are the fees associated with migrating third-party data into the platform?
- ☐ Is there an annual or multi-year agreement required? If so, what is the duration of the agreement?
- ☐ Are there ongoing or additional fees for services such as training, integration, programming automations, customizing questionnaires and maintenance?
- ☐ Are there any other costs that have not been discussed or noted by the vendor?

5.Information Security

Assessing information security is crucial, especially if you are a global organization. With complex and sometimes conflicting regulations concerning anti-bribery, data security and data privacy, it is important to assess how your potential vendors understand and comply with global legislation. At a bare minimum, the ability to pick where data remains should be provided. For instance, with the advent of the General Data Protection Regulation (GDPR), most companies with operations in Europe will desire to store their European data on servers located in Europe.

Any vendor that conducts legitimate business with large multi-national companies is accustomed to working with a client's IT departments and data privacy specialists to complete data security or privacy questionnaires. As important as it may be to retrieve satisfactory answers to such questions, it is equally or even more crucial to ensure that the claims made are regulated and followed. For instance, if a vendor claims to have ISO 27001 certification, request a copy of the certification document and verify it.

KEY QUESTIONS TO CONSIDER

- ☐ What are the vendor's security credentials? What documentation can they provide to support their claims?
- ☐ How is data privacy managed by the platform?
- ☐ What is the platform's authentication system?
- ☐ Is Single Sign On (SSO) available with the platform?
- ☐ On which servers is the information stored? Where are the servers located?
- ☐ What happens to your data should you decide to discontinue using the platform?

6.Demonstrations and Workshops

Demonstrations and workshops are a crucial element in the decision-making process. Demos are ideal opportunities to view a sophisticated representation of a technology at its best. In order to extract as much insight as possible from the demo, first ensure that you clearly understand the steps in your own process and envision those steps and processes working in a system. As you proceed through the first demo, evaluate how the vendor's system would work in conjunction with your processes.

When you are prepared to consider a final buying decision and are attending subsequent demos to further refine your list of potential vendors, ask the vendor to proceed through the platform in a way that imitates your own workflow.

Although most vendors are able and willing to provide sandboxes for potential clients to trial, this experience can sometimes complicate matters. This is because a potential client who experiments with the sandbox system may not be aware of the full functions and calibrations of the system, which may then misinform the client's understanding of the system and provide an inaccurate basis for comparison. If you do request a sandbox, it is advisable to schedule a session where the vendor can guide you through several scenarios and provide documentation to refer to when visiting the platform.

KEY QUESTIONS TO CONSIDER

- ☐ When the vendor proceeds through a demo by imitating your workflow, does the platform demonstrate how it can accommodate for your workflow and processes?
- ☐ Has the vendor walkthrough of the sandbox demonstrated how various scenarios will be handled?

7.Client Success

Picking a vendor is one part of the process. Working with them for a prolonged period of time may, at times, be entirely separate and distinct. Even if a company boasts an impressive sales process, they may not be an effective partner for a long-term relationship. Understand how a company will deliver on the following stages and request an example of the materials presented at each stage:

- ☐ Closing a contract
- ☐ Technology onboarding
- ☐ Post-onboarding calibration of technology
- ☐ Training
- ☐ Regular account management meetings
- ☐ Annual review meetings

By requesting not only what to expect at each stage but also the materials presented, it should be evident which vendors have a rigorous client success model, as well as the people and processes to support it, and which vendors do not.

The price, type and quality of training provided should also be given consideration. As it is in the vendor's best interests that a client knows how to navigate and use the system, training should be included with the platform without extra fees. Online training with an individual who can answer user questions and offer helpful suggestions to using the platform, for example, may be preferred over a user manual by itself. Well-trained users are more likely to maximize the technology's full utility and use it more efficiently.

KEY QUESTIONS TO CONSIDER

- ☐ Does the vendor adhere to a rigorous client success model and offer ongoing support?
- ☐ Are the materials presented at each stage of the process sufficient for your needs?
- ☐ What is the availability of client support systems?
- ☐ What ongoing support is offered for clients?
- ☐ How are new users trained (i.e. through online tutorials, brochures or other means)?
- ☐ What is the availability of IT contacts to assist with technical difficulties?

About Us

Blue Umbrella is a global risk management company specializing in high-quality, high-volume due diligence. Our unique and disruptive approach to third-party compliance has culminated in STATUS, our flexible and user-friendly platform which charges no licensing fees or annual fees for due diligence consumers. We have a global footprint and presence, with operating centers in North America, EMEA, Asia-Pacific and Latin America. We are leaders in providing technology and research to implement a robust system of controls focused on FCPA, UK Bribery Act and other regulatory and reputational risks.

We employ over 250 full-time, in-house research analysts fluent in over 40 languages who conduct research on legally obtainable information for due diligence in both English and local languages. With professional training for researchers and 3-tier quality checks prior to report delivery, our due diligence is of the highest quality.

STATUS, our user-friendly compliance technology, was built by compliance professionals and for compliance professionals to increase efficiencies within your team while relieving administrative burdens. The platform centralizes all relevant third-party information and works to align with your compliance needs, workflows and processes. Our system foundations are purpose-built for third-party compliance and are client-specific, allowing for a high degree of flexibility with automations, workflows, questionnaires, integrations and more. STATUS offers a variety of features such as a robust “rules wizard”, a user hierarchy function and the ability to send and receive various documents within the platform, all of which can be configured with the help of over 50 in-house developers. We are constantly innovating with STATUS, actively integrating with other platforms and scheduling wholesale upgrades so that we can continue to bring you the leading compliance technology on the market for years to come.

Our friendly and professional STATUS support team offers immediate assistance around the globe. Our success team boasts over 16 region-specific client success managers that are happy to assist with any questions, concerns or suggestions you may have and actively work with you to cultivate a positive, long-term relationship.

To discuss anything raised in this whitepaper or how STATUS can help you, please contact:

Allan Matheson, CEO
allan@bluedd.com
+1 778 385 4777

More information on STATUS: www.bluedd.com/status.html