BUSINESS ETHICS
LEADERSHIP
ALLIANCE™
An Ethisphere Community

RISKS, REGULATIONS & REWARDS: THE BUSINESS IMPERATIVE FOR AUTOMATION AND DATA ANALYTICS IN THIRD-PARTY RISK MANAGEMENT

SEPTEMBER 2021

TABLE OF CONTENTS

INTRODUCTION

Emily Rickaby, J.D. M.Ed.
Director, Shared Expertise and Strategic Projects
Business Ethics Leadership Alliance (BELA)
Ethisphere

> “This paper highlights a number of the challenges organizations face in managing third-party risk. It also offers a case for how increased automation, better management of data, and use of data analytics can provide greater returns for both the business and compliance.

If you would like more information about our BELA working groups or other ways Ethisphere or Lextegrity can help you advance your program, please reach out–Emily.Rickaby@Ethisphere.com.

Ethics and compliance leaders today face an increasingly complex set of responsibilities. Risks associated with third parties–corruption, bribery, and other forms of illegal activity–offer a particular challenge. Expectations from the Department of Justice (DOJ) and other guidance suggest that organizations should not only assess risks in onboarding, but also monitor to identify red flags throughout the relationship. It is also expected that companies will use data analytics as part of an overall ethics and compliance program. For ethics and compliance leaders, questions abound. Where do you start? What do you address?

The use of data analytics for ethics and compliance is still evolving. To gain an understanding of the state of analytics for third-party risk management, Ethisphere assembled a working group of senior ethics and compliance leaders who are members of the Business Ethics Leadership Alliance (BELA).

The working group met over a series of months in 2020-2021. Participants spoke candidly about approaches, practices and how this challenge is addressed by the broader business. It was also a time of learning what is possible. Ethisphere’s partner, Lextegrity, showed how new technology can help better automate third-party risk management and apply advanced data analytics to third-party financial transactions for third-party risk lifecycle management. Their expertise and insights shaped the discussion of what is possible in an advanced third-party risk management framework.

This paper highlights several challenges organizations face in managing third-party risk. It also offers a case for how increased automation, better management of data, and use of analytics can provide greater returns for the business and compliance.

We hope you use this paper to learn, and also foster discussion within your organization about ways to improve processes that benefit your organization and your valued third-party partners.

ACKNOWLEDGMENTS

Thank you to the members of the Business Ethics Leadership Alliance (BELA) Data Analytics Working Group for their engagement and contributions that made this whitepaper possible.

Anne Takher, Sr. Director, Ethics and Compliance, Applied Materials

Richard Anderson, Data Analytics Director, Aramark

Tamsin Fast, Chief Compliance Officer, Aramark

Nick Kournetas, Executive Director, Monitoring Analytics and Third-Party Due Diligence, Aramark

Malini Natarajan, Executive Director, Monitoring, Analytics and Third-Party Due Diligence, Bristol Myers Squibb

Nicole Pinard, Global Compliance Monitoring and Analytics, Bristol Myers Squibb

Pamela Liou, Associate General Counsel, Broadcom

Marcello Baruffaldi, Planning & Performance Expert, Embraer

Marina Lofrano, Director, Global Head of Compliance, Embraer

Juliana Venturin, Compliance & Risk Assessment, Embraer

Luz Maria Zea Cabrera, Compliance Officer, Frontera

Jillian Charles, Vice President & General Counsel, Antitrust & Anticorruption, Honeywell

Verity Blair, Enterprise Account Executive, Lextegrity

Parth Chanda, Chief Executive Officer, Lextegrity

Jeffry Garrett, Vice President of Legal, Micron Technology

Scott Sullivan, Chief Integrity & Compliance Officer, Newmont

Gloria Alva, Risk and Operations Compliance Analyst, Peñoles

Manuel Vazquez, Compliance Senior Manager, Peñoles

Tyson Avery, SVP, Deputy General Counsel, and Chief Ethics & Compliance Officer, Starbucks

Cynthia Hill, Corporate Counsel & Manager, Compliance, Starbucks

Andria Kelly, Director Ethics & Compliance, Anti-Corruption, & Investigations, Starbucks

Suzy Quinlan, Manager, Compliance, Starbucks

Laura Velkers, Director, Ethics & Compliance Global Operations, Starbucks

Wafa Derouiche, Vice President and Chief Compliance Officer, TE Connectivity

Brian Risser, Director Legal Compliance and Law Controls, TE Connectivity

Aaron Dutra, Director, Legal Compliance, Uber

Tiffany Scurry, Vice President, Legal and Chief Compliance Officer, Western Digital

THE BUSINESS CHALLENGE

The process of determining which third parties are the right parties to bring onboard—and to keep onboard–often faces stiff challenges from the business if the process is too cumbersome. However, a process lacking rigor can result in heightened risks of enforcement agency actions, monetary loss, and reputational damage. What happens when business and compliance opinions clash over the best way to engage third parties and to manage third-party risk?

It can seem like there's a choice to be made between efficiency and comprehensiveness. There can be a struggle to find the right balance between a one-size-fits-all third-party due diligence process vs. applying a true risk-based model for third-party due diligence and monitoring. Like any other business unit, the Compliance Department desires to work as efficiently as possible, to respond quickly to business needs, and to apply their time and resources to the highest value-add work.

U.S. Department of Justice (DOJ) Guidance

The latest U.S. Department of Justice (DOJ) guidance for the Evaluation of Corporate Compliance Programs (June 2020) makes clear that data analytics are critical:

- Compliance must have sufficient access (direct or indirect) to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions.
- Prosecutors will ask whether there are any impediments that limit access.
- Risk assessments must be based on continuous access to data.
- Continuous reviews should lead to updated policies, procedures, and controls.

Compliance teams are expected to make agile adjustments to programs. This includes periodic risk assessments that track and incorporate lessons learned from a company's own data analytics, reports of misconduct and that of other companies facing similar risks.

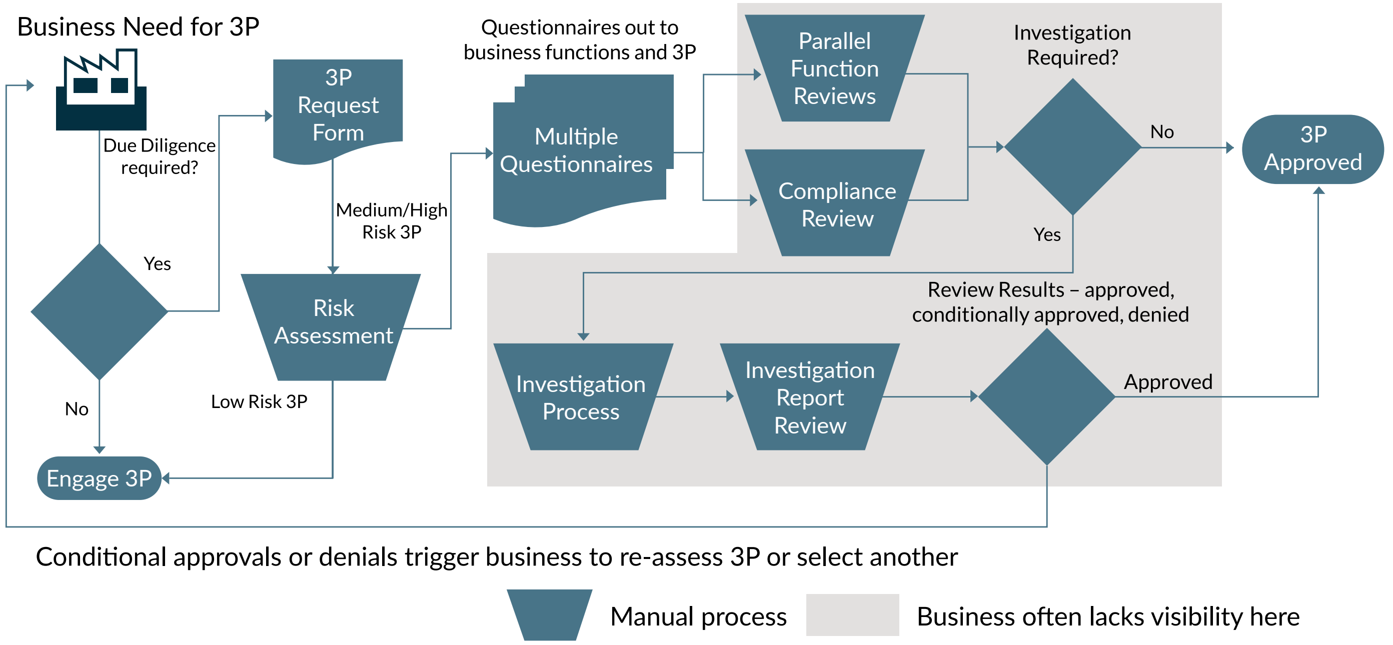
There's no one right way to gain better control and expediency around third-party management practices. There is no fully autonomous silver bullet that addresses every risk or removes the need for human intervention and reasoning. Yet, there are practical steps an organization can take to improve processes that will increase visibility of potential risks and provide benefits to the broader business.

DEFINING THE PAIN POINTS

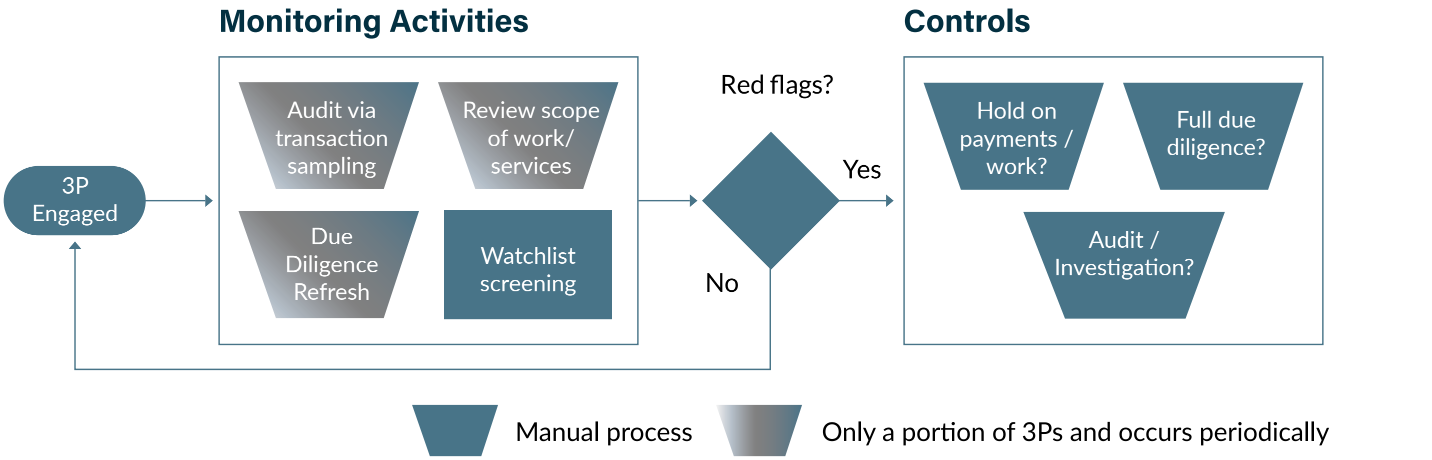
1. Lack of comprehensiveness, accuracy, and efficiency of data

If you look at workflows for third-party due diligence from any number of companies, it is not uncommon to see something that resembles the model below. Some risk assessment processes lead to a portion of potential third parties requiring one or more review and approval processes, including data coming from several sources, a fair number of manual activities, and lack of transparency from the perspective of the business.

Due Diligence Process


Business Need for 3P
Due Diligence required?
Yes
No
3P Request Form
Medium/High Risk 3P
Risk Assessment
Low Risk 3P
Engage 3P
Questionnaires out to business functions and 3P
Multiple Questionnaires
Parallel Function Reviews
Compliance Review
Investigation Required?
No
Yes
3P Approved
Review Results – approved, conditionally approved, denied
Investigation Process
Investigation Report Review
Approved
Conditional approvals or denials trigger business to re-assess 3P or select another
Manual process
Business often lacks visibility here

Reputational monitoring of third parties is often done with ongoing screening against watchlists and periodic due diligence refreshes. Monitoring of third-party transactions is usually far more sporadic and only a small sample of third parties are subject to payment reviews in the course of internal audits. An even smaller percentage are subject to full blown third-party audits.



Issues with data reliability and accuracy can hinder the process even before due diligence

In many organizations, the process often begins with some determination as to whether the third party is even subject to a due diligence process. There is the ubiquitous “garbage in, garbage out” problem when it comes to managing third-party risk. How do you get reliable data in the first place?

There are issues with reliance on end users in the business or third parties themselves to accurately collect or submit scoping or qualification data. Do they have the training and information necessary to identify these initial risks? Are they being fully forthright in the information being provided? In most organizations, this imperfect data can impact the level of diligence done, the level of training provided, and the level of ongoing monitoring conducted on a third party. If the risk analysis is tainted or wrong at the beginning, the downstream impacts can be significant.

Third-party risk management is also a lifecycle risk

Relying on a point-in-time assessment of risk when the third party is being onboarded and has not done any work for the company is a necessary but insufficient control over the entire relationship lifecycle.

DOJ Guidance Note

Risk assessment should not be limited to a “snapshot” in time. Aim for continuous access to operational data and information across functions.

A “low-risk” vendor may have sidestepped the diligence controls and may actually be “high-risk,” or may become “high-risk” over time as their scope of work changes. For example, a marketing consultant may begin by creating content and then later expand to interacting with state-owned media to garner positive press coverage for the company.

Multiple touchpoints and lack of integration of processes can create gaps

There could be many touchpoints throughout the business for a given third party. How do you collect and integrate all of the information that exists around the company? Local resources can have valuable information about a third party. How do you gather this information efficiently? Manual use of spreadsheets, multiple questionnaire sets, and subjective reviews leave gaps where risks can develop, and the business can get bogged down.

Having risk assessment information spread out over multiple functions can also create due diligence fatigue, which only increases the odds of inaccuracies and makes taking short-cuts more attractive. How do you achieve comprehensive due diligence without halting the business?

Highly manual processes cannot scale

Merger and acquisition (M&A) activity also creates headaches in the area of third-party management. Manual diligence processes cannot scale as volumes increase. The acquired entity may bring additional systems, tools, and processes along with data that is inconsistent with the acquiring entity or even inconsistent within its own environment. This can create layers of complexity during pre-M&A due diligence and post-close integration.

2. Lack of consistent and updated risk-level definition or risk-based processing

Organizations often struggle with developing risk scoring methodologies

How do you define risk levels? How do you weigh individual risk levels or combinations of risks? Should organizations look to industry standards? How do you get this right?

DOJ Guidance Note

Companies should apply risk-based due diligence to its third-party relationships.

One set of categories in determining risk levels might be critical vs. non-critical parties, but what do you do with high risk but critical third parties? What about flaws in existing risk classifications, perhaps taxonomies of classifications in legacy systems or tools, that create fuzziness as to if a party is in or out of scope for a particular level of review? This can lead to manual review of all third parties, bottlenecks, or longer periods for review.

What about regulatory issues that run counter to the level of due diligence you are trying to achieve? For example, in a jurisdiction where it is not mandatory for a company to reveal their end beneficiaries it would be hard to draw conclusions about risk if the disclosure is not available. A similar issue presents itself with regulations on data privacy rights that may run counter to disclosure requests. How do you incorporate information on regulations that might run counter to your due diligence requirements as part of the risk scoring process where this may trigger the need for enhanced due diligence?

Third-party risk classifications deserve closer attention

Some companies find themselves relying on legacy classifications of third parties and risk levels. They may be bound by the taxonomies in existing systems and face inconsistencies among these systems. Business users may also be unable to appreciate nuances in these classifications, such as whether the third party is acting on behalf of the company with respect to government officials. The business may be unclear whether the third party is truly an agent or may have a narrow interpretation of who is a government official. There could also be confusion throughout the business about the identification of a government-facing third party vs. a third party that presents a commercial bribery concern and could be high risk under the anti-corruption program overall.

3. Lack of transparency and inconsistent controls and monitoring

Decentralized processes can lead to inconsistent controls

In some organizations, third-party risk may not be managed under a centralized process or by one function. Compliance does not own all the risks or processes for due diligence. For example, a company could have a pool of third parties associated with the buy side (e.g., vendors) vs. the sell side (e.g., distributors and resellers) and those relationships may be managed in different systems (e.g., a procurement system for the former versus a customer relationship management system for the latter). There may be joint responsibility between Compliance and other functions for certain regulatory compliance risks like health, safety and environmental issues in manufacturing or GxP (good practice and standards) in pharmaceutical or life sciences businesses.

It can be hard to find a solution that works for multiple segments of the business, and consolidation could require a change for multiple legacy workflows and processes. Different business units may be running on different ERP/financial systems, leading to multiple onboarding processes and making it more difficult to integrate data into one source. However, Compliance can often set the scope and strategy even if other functions are carrying out the risk management or due diligence processes.

Clear line of accountability and authority is key but often lacking

Who owns the decision to bring on a third party? Is Compliance an advisor? Or the decider? Some organizations are shifting the diligence process to the front end and to the business. For example, asking the business to chase the vendor to get the information before it comes to Compliance for review or after Compliance does an initial screen and determines a need for additional information.

DOJ Guidance Note

Companies should know the business rationale for needing the third party.

When is it appropriate to use an exception or conditional approval of a third party? How do you set the rules to make sure that even if you authorize use of the third party under an exception, you get the information you need in a timely matter to complete the screening?

There is a need to document and record the enhanced due diligence process including the business rationale to support the use of a higher-risk third party. Could a proper system flag third-party outliers and provide better awareness as to where this exception is in terms of follow-up on documenting the business case for the use of the third party?

A GLOBAL DISRUPTION PROMPTING LASTING CHANGE

The pandemic has been the most disruptive event of our lifetime. Business continuity became an issue. Suppliers went out of business or became inundated. Companies had to pivot their strategy to survive. It also exposed and increased third-party risks that remain today:

- **Economic pressures creating opportunities for corruption.** Emergency public procurement and shortages of key equipment and the expectation of 'rapidly deliver above all else' increased the incentives for wrongdoing.
- **Change in processes**, with fewer on-site visits and face-to-face discussions.
- **Disrupted supply chains** resulting in the need to quickly onboard new vendors, with manual due diligence processes that don't keep pace.
- **Disaggregated working environments** that make it more difficult to detect suspicious activity.

At the same time, companies are now more vulnerable than ever to enforcement and a growing raft of legislation. Specifically:

- **An increase in anti-corruption regulations** and liability for companies with supply chains extending across many businesses and jurisdictions. In addition to the US, UK, French, and Mexican governments, more and more countries are implementing and updating their own anti-bribery laws with broader scopes and stiffer penalties.
- **A rise in enforcement actions** based on third-party activities. Not only is legislation being enforced more often, but the size of fines is growing too. Global regulators are now working more closely together to enforce regulations and are handing out multiple fines for the same infringement.
- **Expanded scope of FCPA investigations.** It is no surprise to see US-based organizations facing the brunt of FCPA investigations. But organizations headquartered in Germany, Sweden, Switzerland, and The Netherlands–all of whom ranked among the top 10 countries in Transparency International's most recent Corruption Perceptions Index–are featured prominently in recent FCPA investigations and the Bribery Payer Index (BPI).

Falling afoul of the regulations can result in huge fines and financial penalties. But there are more significant and long-term costs to bear in mind. These include reputational damage, share price drops, negative impact on the ease of doing business, as well as ongoing legal and monitoring costs. It is easy to refer to fines for wrongdoing. Often overlooked are the legal costs, costs realted to remedial measures and ongoing monitoring costs, as well as disruption to the business and damage to an organizational culture, which for many organizations will dwarf the cost of any fine.

Robust compliance programs and proactive due diligence can lead to credit from law enforcement agencies and help reduce penalties through vehicles such as Deferred Prosecution Agreements (DPAs). With large penalty discounts available for taking prudent action, the message is clear: companies that invest in effective compliance controls will be treated more favorably than those who do not do so.

EXPLORING AUTOMATION AND DATA ANALYTICS

Digital transformation of third-party due diligence and monitoring activities holds many benefits for a business. Automation and data analytics tools can improve processing time, reduce risk exposure, streamline approvals and controls, allow for continuous monitoring, and provide the business with a more accurate picture of current third-party activities.

The question for many is, what should automation and data analytics solutions include? A few pointers:

Onboarding

- **Embed automated and objective risk assessment** into the vendor onboarding process to minimize human judgment (e.g., automate a scoring algorithm that reduces the judgment an employee needs to apply to the third party).
- **Integrate complex approval logic** for requests to trigger appropriate approval based on risk factors, functions and/or policy criteria so that processes can be better tailored to the risk.
- **Further leverage automated questionnaires** with branching logic (additional questions based on prior answers), and the ability to capture policy attestation, and to send back and forth questionnaires within a technological platform. This approach enables easier collaboration between the business and third parties to ensure higher rates of completed questionnaires. It also reduces completion times.

Ongoing Monitoring

- **Tie vendor onboarding risk assessment results to ongoing monitoring** efforts in an automated fashion.
- **Automate analytics and reporting** by business user, business unit, country, and region to identify outliers and opportunities for risk reduction.
- **Monitor transactions in real time**, instead of a sample on a periodic basis via audits and other ad hoc monitoring.
- **Expand monitoring** beyond sanctions and watchlist screening to continuous monitoring of all third-party financial transactions or changes in scope of work.

Taking these actions provides a range of business benefits:

- **Protect the business from process or judgment errors** by automating risk determinations.
- **Save time by making the onboarding process more efficient** by targeting compliance resources to the highest risk third-party engagements.
- **Manage risks more closely on an ongoing basis** to detect changes in scope or risk and identify risks before they become systemic.
- **Provide business leadership with risk data to own risk decision-making** more effectively (e.g., manage their own supply chain risk better).
- **Enable cleaner third-party master data** within the organization and less manual data entry for existing third parties.
- **Strategically streamline third parties** based on risk data to save money and reduce risk exposure.
- **Better protect the business from a growing raft of legislation** and enforcement action.

Compliance teams can also realize a range of program benefits:

- **Provide more stringent and objective controls** in the onboarding process.
- **Validate the effectiveness of third-party onboarding** controls by cross-referencing initial risk determinations against financial transaction risks.
- **Provide more global and holistic lifecycle risk** coverage by monitoring 100% of third-party financial transactions using sophisticated data analytics.
- **Prevent and detect issues** and anomalies before they become systemic risks.
- **Provide better visibility** across the entire third-party population, to inform learning and further maturation of processes.
- **Embed intelligent end-to-end workflows** using technology to ensure a better user experience for the business as well as a full audit trail.

Harmonizing processes and systems drive effectiveness and efficiency

Harmonizing and automating these multiple siloed processes into one platform or technology can make the process far more effective and efficient. Having configurability to set risk scoring based on information the company already holds, from its own risk assessment exercises for example, is essential for a truly risk-based approach to due diligence.

More effective use of post-engagement data analytics can also serve to shift the balance of enterprise efforts between the front-end onboarding process and renewal due diligence, and the back-end monitoring process.

Minimizing subjectivity can help with bias and information gaps

By better automating and embedding risk determinations, a company can remove some of the subjectivity of the risk assessment process to better target onboarding efforts. Data analytics on third-party financial transactions can then be used to detect risks in the actual financial transactions from the first day of using a third party and beyond, so if corners were cut or information was incomplete in the onboarding process, those variances in risk profile could be detected quickly and remediated.

> The front-end controls, questionnaires and processes could potentially be streamlined if more holistic back-end monitoring is implemented.

Scale and prioritize M&A review to higher risk areas

The M&A context is an ideal use case for data analytics. The acquisition target may have a large supplier base, some of which are duplicative of the acquirer and some that may pose significant compliance risks.

The traditional approach of manually and subjectively assessing those suppliers over a long period of time and onboarding those third parties anew via the acquirer's due diligence process can be cumbersome and imperfect. Instead, data analytics could be applied to the target's spend data to identify the highest risk third parties for closer due diligence inspection.

DOJ Guidance Note

Companies should not spend disproportionate amounts of time policing low-risk areas instead of high-risk areas.

A data analytics exercise could also provide objective data for business stakeholders to make commercial decisions around rationalizing third parties to both save money and reduce compliance risks.

Risk scoring is a dynamic process; not "set it and forget it"

Ensuring that your risk categorization is highly configurable is key to a truly robust and dynamic third-party risk management process. The DOJ guidance cautions against snapshot risk assessment and that applies directly to third-party risk management.

Your data analytics should be periodically feeding your risk scoring methodology. For example, a hot spot may show up in your spend data in a traditionally low-risk country or for a traditionally low-risk service category. This should then feed changes in your upfront diligence model in more of a real-time way.

Data analytics on spend data can serve as a powerful harmonizer of risk information because the same analyses are being applied to all third parties globally, so you can now compare third parties to one another uniformly using objective data analyses. Learnings from this exercise can help you improve or better harmonize antiquated front-end due diligence methodologies.

DOJ Guidance Note

Companies should have mechanisms to ensure that contract terms describe the work performed, that the payment terms are appropriate, that the contractual work is performed and compensation is commensurate with services rendered.

Silos may remain, but in a better-managed state

As stated previously, Compliance does not necessarily own all the risk management or due diligence processes around third parties. You should be clear about "what kind of diligence or what types of risk are we looking to manage with an automation or data solution?" It may not be possible to completely deconstruct due diligence functional or process silos (e.g., anti-corruption, global trade, data security and privacy, ESG, human rights, conflict minerals, et. al.) in many organizations. In such cases, compliance teams should look for opportunities to connect a centralized compliance process to those disparate functions and their related systems. So, if vendors are added via a procurement system and distributors are added via a CRM system, the compliance due diligence process should be connected in some manner into both of those processes..

For example, a completed compliance due diligence approval might be required for certain vendors and certain customers to proceed in those systems. In addition, if during that process, Compliance, Privacy and Global Trade need to opine on the third party, harmonizing their efforts into one platform should be a long-term goal of the organization. Doing so both streamlines and better controls the review and provides efficiencies and a better user experience for the business.

The human factor: still the biggest component of any successful technology implementation

Change management hurdles and matrices within organizations can make it difficult to achieve a vision of harmonization across third-party risks.

Companies often experience one of the following when trying to do this:

1. Companies that want to harmonize everything at once.
2. Compliance wants to harmonize but other functions are not on-board.
3. Compliance has buy-in but they do not have the solution selected or the roadmap in place to make it happen.

As mentioned, different aspects of due diligence may be done by different functions so thought should be given to how to manage and coordinate those processes even though they may need to remain separate. In such cases, working to strengthen the controls in each area could be the medium-term goal. Or perhaps a beneficial exercise for companies would be to better define the universe of due diligence activities. Compliance could be the one to provide a framework, but there is still the need to define business roles and develop the business rules with input from key functional areas.

> Defining third-party risk across the company is sometimes the hardest part of readiness to move toward a technology solution for third-party management.

Stories from the working group

> *We took the approach of defining the scope of the work by starting with smaller subsets of third parties or higher risk entities or activities. We used these subsets to break the work into manageable pilots first instead of trying to tackle the full range of third-party due diligence activities.*

> *The business and regulatory risks created the motivation for us. We were seeing issues arise and everyone understood there was a need to do something. We involved the business throughout–everyone has a role–and we all needed to have the same risk mindset around the process.*

> *The project was more of an administrative and process-centered lift vs. a technical effort. We needed to define and set the rules for risks and then map types of third parties to those risks. After that we were able to start looking at what types of data are needed to perform assessments based on those risk definitions. All of this varies for different types of third parties. But this process was integral to determining who owns what and who does what as far as the relationship with and management of the third parties. This process took 12 to 18 months.*

Many companies will get approval and resources for new technology but struggle with getting it implemented. You need to get the right people at the table. There is work to be done on process analysis, definition and refinement of business roles and rules, and creating the necessary and often new workflows required to implement new technology. Managing expectations can be very hard with senior leadership. You will need to focus on the process while contemplating a technology solution, and the maturity of your technology solution may enable your enterprise to realize a better process.

HOW TO GET STARTED

It can be daunting to think about initiating a data analytics journey. Here are a few steps to get going.

Process and workflow review

Assess processes and business rules.

You don't want to simply automate an inefficient, unnecessary or ineffective process. Take the opportunity to root out non-value add or duplicative steps in your process and validate the business rules that drive them as a part of your data analytics and automation project. Work with the business to create a process that they can own.

Focus on processes that are most value add.

The immediate goal is not to automate all processes and achieve operational perfection. Consider those that can give you and the business greater insights.

Determine where manual intervention is still required.

Engage the business in this process from the beginning.

Consider data analytics when other systems are up for review.

If your current due diligence process is being assessed or your current platform provider is up for renewal, use the opportunity to assess whether smarter automation processes are possible. This provides an opportunity to build success there along with access to necessary data, then use that success to move forward to pool additional data to enhance monitoring and controls practices.

Consider ways to build on existing systems.

If you already have a basic third-party diligence process, you could also shift your attention to better monitoring using data analytics, as this is the largest gap in most organizations. This can help you better understand where/how the business is using approved third parties and provide relevant, reliable, and useful information for both the business and compliance. It can also inform revisions to the front-end due diligence process in the longer term.

Have a vision for what data you want to report out on.

Determine what metrics matter to Compliance and to the business. Some examples include:

- Average risk score of third-party financial transactions per country
- Third parties ranked by financial transaction risk scores versus spend amounts
- Average time (days) to onboard a third party
- Length of time to process a renewal
- Duration of each step of the process
- Percent of approvals or reviews completed within a target timeframe
- Number of denied parties across segment and business unit
- Red flag rates

Identify necessary data

Don’t spend time, money or effort on data that is not needed or doesn’t add value.

Map your processes against the risks you are trying to mitigate and see which steps and activities support or add value to that risk mitigation and which steps you can eliminate or might be duplicative of other process/activities.

Look for economies of opportunity.

You don’t have to access every system and all data; you can make improvements and gains even in a diversified/decentralized data environment.

Understand that access to data can also be overwhelming and counterproductive if not properly targeted.

Spot analytics (e.g., all round currency payments) and outlier visualizations (e.g., the highest paid vendors in a market) can lead you down the wrong path or paths of little value. Concentrating more on applying multiple risk analytics to each financial transaction and then aggregating those results at the third-party level can focus your review on the highest risk transactions or third parties.

Clearly articulate the needs and benefits

Have a clear vision that you can share with the business.

Give the broader base of stakeholders something to buy into and allow them some ownership of the risks involved with onboarding new third parties, and as is often overlooked and underestimated, managing ongoing risks related to existing third parties.

Build your business case on efficiencies,

not head count reduction. Focus on better coverage, capturing more true red flags, and the ability to focus where manual effort should be applied to higher risk activities.

Demonstrate how this supports regulatory review

and building a defensible program.

Consider a phased approach to digitization.

Partner with the business to determine the path forward.

Get the right experts at the table.

Third-party risk has many stakeholders, and if you have buy-in from the relevant departments on the objectives and benefits that will come with proposed changes, the change management process will be easier.

Assess solution providers.

- Get references and talk to peers that use the products.
- Make sure the solution matches the scope of risks you need to manage today and in the future (e.g. can your due diligence approval tool also support data analytics on financial transactions).
- Understand the track record and the long-term vision for any vendor around supporting the entire breadth and lifecycle of third-party risk, and the odds that the company will be around for the near future.
- Not all solution providers offer services to guide you through the process of implementing their solutions. Understand what is included as part of the solution.
- Some providers might not offer customization that a company envisions, or the customization might come at a cost (monetary or development time).

Bring key functions into the vendor review.

- Connect with your Procurement or Sourcing teams for their insights about any potential solution provider.
- Include IT to understand if a given technology will work within your company's technology ecosystem and strategy, and to look for solutions that may be available from vendors you are already using.
- Consult with Finance and Accounting to understand the connections or potential connections with your accounting systems.

CONCLUSION

Third-party risk management is a challenge that spans across an organization and involves a range of stakeholders. Ethics and compliance leaders face increasing pressure from regulators and others to ensure integrity among third parties. Data analytics offers a way to streamline processes and gain increased transparency across the value chain with a benefit to all.

In the end, it is about building a defensible program that can evolve over time in response to lessons learned in a fluctuating environment. This paper has presented a number of questions to guide compliance leaders to assess the state of third-party risk management within their programs and with various business functions in their organization. Knowing which questions to ask is a first but necessary step on the path to understanding what tools and systems will be of benefit to the specific risks of your organization.

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

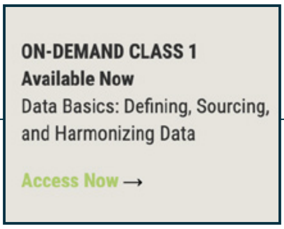
ADDITIONAL RESOURCES

Learn more about the role of data analytics in ethics and compliance.

Webcasts

On-Demand Webcast Series

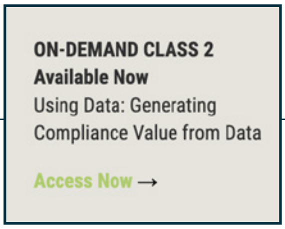
Learning Sessions for Ethics & Compliance Leaders Looking to Leverage Data Analytics to Improve Programs


ON-DEMAND CLASS 1

Available Now

Data Basics: Defining, Sourcing, and Harmonizing Data

Access Now →


ON-DEMAND CLASS 2

Available Now

Using Data: Generating Compliance Value from Data

Access Now →

ON-DEMAND CLASS 3

Available Now

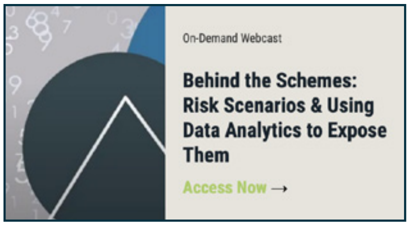
Practical Data Analytics: Deep Dives Into Specific Use Cases

Access Now →

On-Demand Webcast

Using Data Analytics to Improve Ethics & Compliance Program: A Practical Roadmap

Access Now →


On-Demand Webcast

Behind the Schemes: Risk Scenarios & Using Data Analytics to Expose Them

Access Now →

Infographics

Infographic

Traditional Auditing vs. Continuous Monitoring

Download Now →

Infographic

How Data Analytics Can Transform an Enterprise

Read More →

Infographic

Top Five Ways to Exceed the DOJ Guidance

Read More →

Articles

Article

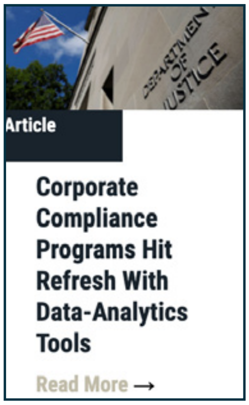
Tips for Detecting Pandemic Fraud Risks

Read More →

Article

Third-Party Risk Management with Data Analytics

Read More →



Article

Corporate Compliance Programs Hit Refresh With Data-Analytics Tools

Read More →