Third Party Risk Management in the Age of Big Data and Advanced Analytics

Incorporating Advanced Technologies into Third Party Programs to Mitigate Third Party Risk and Satisfy Regulatory Requirements

A WHITE PAPER FROM SURVEILLENS

October 2017

Contents

Introduction

As organizations continue to grow their business operations with the introduction of new products, additional services, and expansion into new jurisdictions, compliance and legal officers are facing increasing pressures to manage risks from new and existing third-party relationships, some of which can be dangerously complex.

Global regulators have repeatedly stressed their views on the importance of managing third party risks by requiring implementation of robust third party due diligence programs that include robust policies, procedures and controls designed to mitigate third party risk.

Such programs would benefit from the adoption of advanced technology solutions such as big data platforms and predictive analytics. Advanced technologies have fundamentally altered the way companies approach risk by dramatically reducing the cost and time associated with harnessing multiple data sources, managing, and conducting due diligence on third parties. Implemented properly, they also serve to streamline ineffective and inefficient due diligence and risk management procedures such as one-time searches, manual, outdated, and one-size fits all approaches, and delivering timely and meaningful insights that allows compliance and other personnel to remain appropriately informed.

This white paper will discuss the risk presented by third parties, the components of an effective third-party risk management system, limitations of current third party systems and finally, how platforms powered by advanced technology solutions such as big data analytics, artificial intelligence, natural language processing, and social network analyses can assist organizations by minimizing expensive outsourced due diligence, streamline data management and decision making and, in turn, achieve effective regulatory compliance.

Vijay Sampath, CEO
surveilLens

The Importance of Third Party Risk Management

While third party risk has been a legal and compliance requirement for quite some time, in recent years the growing complexity of third-party relationships, combined with the regulatory and reputational risks posed by those third parties has compliance officers and legal departments struggling to determine the best way to manage their third-party risk.

Third party risk can come from third parties whom the organization uses to obtain products and services such as vendors, suppliers, service providers, resellers, distributors, business partners, agents, consultants etc.

Third party risk management has become a hot button topic in recent news as the headlines have been dominated with stories of companies penalized for compliance failures resulting from relationships with criminals, politically exposed persons (PEPs) or other individuals that expose the organization to fraud, compliance, legal or regulatory risk.

> *Over 70 percent of FCPA actions involve the actions of third parties*
> *Karen Brockmeyer – Chief – SEC FCPA Unit*

> *Risk-based due diligence is particularly important with third parties and will also be considered by DoJ and SEC in assessing the effectiveness of a company's program.*
> *Source: Resource Guide to the U.S. Foreign Corrupt Practices Act – U.S. DoJ and SEC - November 2012)*

Aggressive enforcement of new and existing regulations has resulted in legislation across a variety of industries making it clear that regulators are placing an increased emphasis on compliance and third-party diligence programs as a means to prevent fraud and other misconduct committed by or against organizations.

Recent Department of Justice (DoJ) and Securities and Exchange Commission (SEC) enforcement actions related to violations of anti-bribery laws such as the Foreign Corrupt Practices Act (FCPA) and U.K. Bribery Act have shown that there is a direct link between the strength of an organization's due diligence efforts and program and corruption. These actions further demonstrate that third parties, including agents, consultants, and distributors, are commonly used to conceal the payment of bribes to foreign officials in international business.

Third party risk can also come from an organization's customer. The financial services industry is particularly sensitive to this fact. As the first line of defense in the continual fight against money laundering, banks and other entities deemed to be financial institutions, are subject to increasingly stringent and extensive know your customer (KYC) protocols over their customer base. Due diligence requirements in U.S. domestic

legislation such as the Bank Secrecy Act (BSA), U.S.A. PATRIOT Act, Foreign Account Tax Compliance Act (FATCA) continue to be strictly enforced resulting in billions of dollars of fines to the institutions that are found to be in violation. Nor is the U.S. government alone in stressing due diligence protocols. In Europe, the Fourth and Fifth European Union (EU) Anti-Money Laundering (AML) Directives (4AMLD and 5 AMLD) as well as the new French anti-corruption law, Sapin II, also mandate the implementation of procedures for conducting due diligence on clients, suppliers and third parties.

So important is due diligence, that the U.S. Federal Sentencing Guidelines, which include "performance of due diligence to prevent and detect criminal conduct" as an integral element of an effective compliance program, provide organizations with credit against fines and penalties for maintaining an effective compliance programs in the event alleged misconduct is discovered.[1]

Relevant Legislation for Financial Institutions Requiring Due Diligence

Legislation	***Requirements***
4AMLD & 5AMLD (EU)	• Member states required to obtain and hold adequate, accurate and current information on corporate and other legal entities, including trusts and similar legal arrangements, incorporated, or administered within their respective member state.
Bank Secrecy Act (FinCEN)	• Requires financial institutions to establish and maintain written procedures that incorporate the identification of beneficial owners of legal entity customers into their AML compliance program. • Strengthens customer due diligence (CDD) requirements and unofficially incorporates CDD into a new fifth pillar for BSA/AML programs. • Elements of CDD o Identifying & verifying the identity of your customers. o Identifying & verifying the identity of beneficial owners with 25% or more equity interest of your legal entity customers. o Understanding nature & purpose of customer relationships. o Conducting ongoing monitoring to maintain and update customer information & to identify & report suspicious transactions.
USA PATRIOT Act	Section 312 – requires financial institutions to perform due diligence, and in some cases, enhanced due diligence, with regard to correspondent accounts established for maintained for foreign financial intuitions and private banking accounts established or maintained for non-U.S. persons. Implements general due diligence requirements pertaining to foreign financial institutions.
FATCA	Banks required to provide information to the IRS about accounts owned directly or indirectly by U.S. persons, as well as foreign entities that are not properly documented with a U.S. tax form.

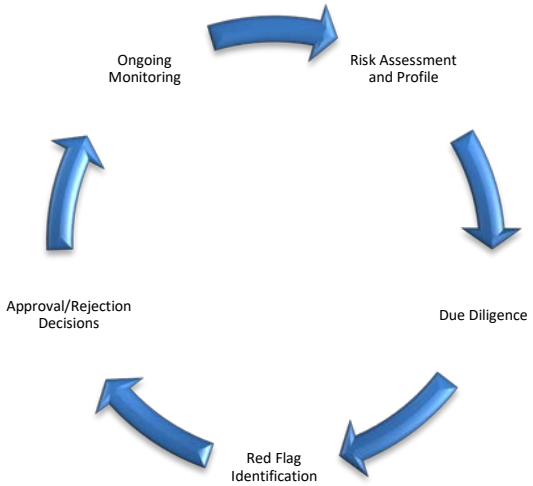
[1] U.S. Sentencing Commission, Federal Sentencing Guidelines Manual, Chapter Eight "Sentencing of Organizations – Part B – Remedying Harm from Criminal Conduct, and Effective Compliance and Ethics Program," 8B2.1 Effective Compliance and Ethics Program (a)(1), available at http://www/ussc.gov/Guidelines /2011_Guidelines/Manual_HTML/b82_1httm.

As a result of the aforementioned regulatory activity, organizations have recognized the need for maintaining robust third-party management procedures as part of their overall compliance program. Such procedures will typically include due diligence on business partners, vendors and other third parties as well utilizing a risk based approach to proactively identify corrupt behaviors.

Designing a Program to Manage Third Party Risk

The process of establishing and maintaining a third-party compliance program can be a challenging task, particularly for larger entities who may have upwards of thousands of relationships around the world. Accordingly, it behooves organizations to have formal documented due diligence policy and procedures that seek input from other relevant groups in the organizational chain of decision making.

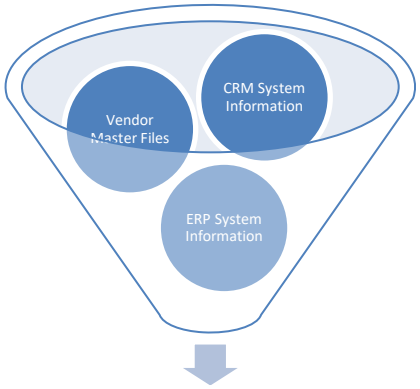
Third Party Risk Management Program



Conducting the Risk Assessment and Developing the Risk Profile

The starting point of a well-managed and maintained third party compliance program begins with a risk based approach that classifies third parties based on their risk profile. While the risk assessment process can take many forms, the most common process begins with consideration of certain minimum factors such as:

- the background of the third party and its owners if the third party is an entity,
- the third party's relationships, with government entities,
- the nature of the third party's operations,
- the use of agents, consultants or other intermediaries,
- jurisdictions in which the third party operates.



Third Party Risk Assessment

Information for the risk assessment can be obtained from multiple sources within the organization including customer and vendor master files, customer relationship management systems and prior transactional histories recorded in enterprise resource planning (ERP) systems. Once relevant information sources are identified, there may be some effort required in gathering and organizing them for proper analysis and risk classification (e.g., low, medium, high risk). At this stage the organization should also consider the use of key risk indicators (KRIs) associated with each third party and the appropriate weight to be assigned to each developed KRI in the risk assessment process. Higher risk third parties are given priority in the organization's due diligence efforts.

Due Diligence

Following the development of initial risk profiles, due diligence on each third party should commence. The level of diligence can vary based on the level of risk assigned to the party. Thus, diligence on lower risk parties would consist of minimal procedures such as review of publicly available information (e.g., media and litigation databases) while medium and high risk third parties may require enhanced due diligence (EDD) techniques such as a physical review of the third party's operations (i.e., boots on the ground research). Regardless of the nature and level of research conducted, the organization should take steps to ensure that the process is fully documented in the event that the nature or level of diligence is ultimately questioned or reviewed by a regulatory agency. Finally, negative or adverse information learned from the current due diligence efforts, should be incorporated as a KRI in future risk assessments.

Sample Due Diligence Procedures Based on Third Party Risk Classification

Low Risk	*Medium* Risk	*High Risk*
•Searches of media and publicly avaialble information (e.g, watchlist databses etc.) •Completion of due diligence questionairre by third party •Third party ceritfications	•Low risk procedures + •Interviews + •Review of third party financial information, e.g., bank statements	•Medium risk procedures + •Physical review of third party operations (i.e., boots on the ground)

Red Flag Identification

As a result of the risk assessment and the diligence process, the organization may identify "red flags" associated with individual third parties which will either require additional due diligence or, if severe enough, disqualify the third party from doing business with the organization. Common red flags that may give organizations pause include:

- Third parties or members of the third-party organization associated with PEPs
- Third parties subject to current or previous inquiries or actions from regulatory bodies

- Negative news media associated with the third party
- Prior criminal history of the third party.

Approval/Rejection Decision

Based on the organization's review of the diligence and any red flags, it must decide whether to approve or reject the third party being reviewed. Consistent with other steps in the process, the process behind any final decision, particularly decisions made to approve third parties notwithstanding the existence of red flags, should be documented and maintained in a file by the organization's Legal or Compliance department.

Ongoing Monitoring

Ongoing Monitoring Based on Third Party Risk Profile

Low Risk	*Medium* Risk	*High Risk*
•Searches of media and publicly avaialble information (e.g, watchlist databses etc.) •Completion of due diligence questionairre by third party •Third party ceritfications •Performed at orgnization's discretion	•Low risk procedures + •Interviews + • Long range audits •Performed at orgnization's discretion	•Medium risk procedures + •Onsite audits •Physical review and confirmations •Performed at orgnization's discretion but no less than annually

Once a business relationship is established, the steps in the risk management process should be performed on a periodic basis to ensure that subsequent events or information lead to changes in the initial risk profile or KRIs and individual third parties or in the risk process as a whole.

Practice Tip: Audit rights included as part of third party contracts are an effective means of completing the ongoing monitoring step. The nature and extent of the actual audit procedures conducted will vary depending on the risk profile of the third party.

Organizations should determine the appropriate amount of time between reassessments. Consideration may also be given to staggering the time between reassessments based on risk profiles. Best practices however, dictate that reassessments occur at least annually for medium and high risk third parties.

Limitations of Third Party Risk Management Programs

Fraud schemes are not dynamic and will change over time as fraudsters continue to seek ways to trick companies into doing business with them. Regulators, no longer satisfied with "check the box" compliance, expect organizations to be proactive in their CDD efforts. As such, maintaining a current CDD compliance program that considers domestic and international due diligence requirements can be complex and even worse, expensive, if improperly implemented.

Many third-party programs however fail to live up to expectations regardless of the number of internal or external resources thrown at the problem. Issues stemming from the use of out dated methods, to the failure to identify, extract and integrate relevant data, result in many programs failing to capture and present data promptly and in a meaningful fashion to decision makers and thus become an ineffective component in an incomplete compliance program.

Use of Manual Techniques

Many organizations continue to rely on outdated techniques, such as manual processes to satisfy due diligence requirements. Manual diligence techniques however, are often decentralized, ad hoc and fail to incorporate and consider all relevant data resulting in incomplete analyses and redundancies all of which ultimately prove to be unnecessarily costly and time consuming.

> *According to a recent survey of banks, KYC systems were the 10th oldest systems in terms of installation date within surveyed organizations.*
> *Source: CEB 2016 FSI survey*

Furthermore, manually sifting through massive amounts of data produced by various sources in disparate formats to determine what is relevant for purposes of analysis can be time consuming and costly. Humans can only process a limited amount of data before they get tired or distracted during their duties thus causing their review of data to be subject to errors or even worse, to miss a crucial piece of information related to a third party.

Use of Outdated Technologies

Even in instances where the organization relies on automation in its third-party program, these systems may be outdated or unable to fulfill the demands of modern day regulations.

For instance, organizations often experience issues associated with poor quality, importing and integration of such data into existing digital channels. Different entities or

units within the organization may be operating under legacy onboarding systems that lack the flexibility required for integrating and interfacing with modern day diligence systems. As a result, many institutions spend more time preparing data than actually using it to assist in making time sensitive decisions.

Inability to Identify or Access Relevant Data

Data siloing can also be a primary source of inefficient and costly third-party programs. Data is often stored not in one easily accessible database, but across many areas such as customer relationship management software, in personal spreadsheets or, in some cases, employees' minds. Accordingly, rather than facilitating a holistic or single view of each third party, such siloing can lead to issues of redundancy of data for the same customer or conversely, conflicting, or missing information in records

Dealing with False Positives

Automated solutions often fail victim to the problem of being overly inclusive; that is resulting in too many potential matches. Whether due to overly broad rules, improper thresholds, or failure to properly understand processed data, most solutions generate an excessive amount of false positives. Organizations however, do not have the time, capacity, or financial resources to investigate each potential match that could be related to the third party on whom they are conducting due diligence. False negatives, can be equally, or more troublesome. Failure to identify a sanctioned entity, or third party with a link to terrorist financing due can lead to severe financial penalties and reputational risk.

Many simple automated solution face issues because they fail to standardize watchlist and third-party data entries that include inconsistencies, inaccuracies, or are incomplete. Screening against data that is not fit for purpose reduces screening accuracy, and thus increases risks and costs. Accordingly, name and address standardization is of extreme importance when it comes to recognizing which details belong to the same entity and which denote separate ones altogether.

Example

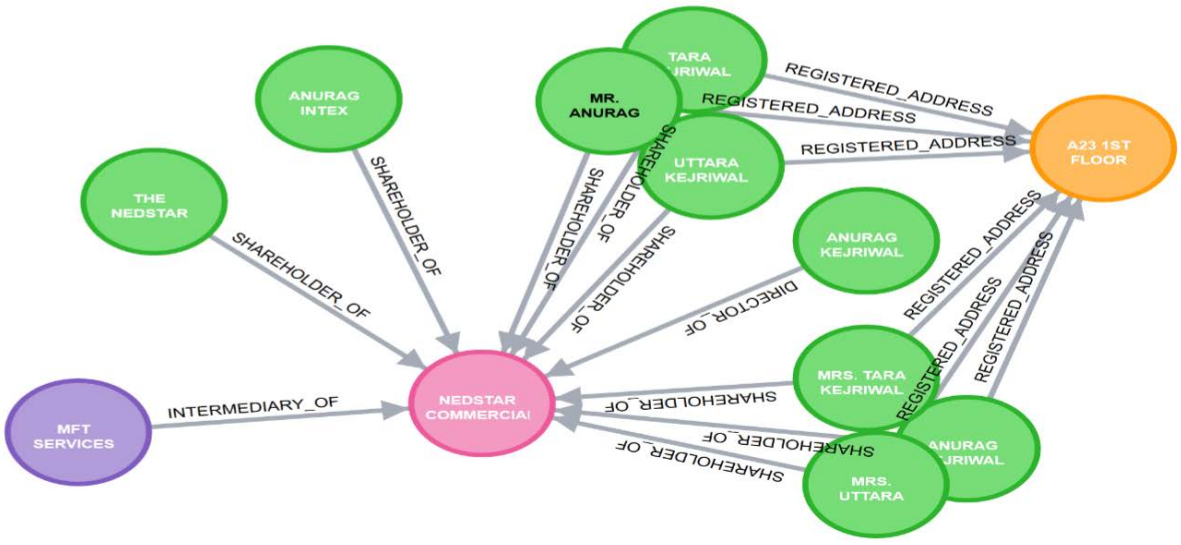
Bank X has 15 accounts each with a customer named Robert Smith, Bob Smith, R. Smith, or B. Smith. The challenge thus becomes determining whether there are one, two or 15 customers of the same name—and if the totality of transactions on all accounts trigger an alert or reporting obligation. For instance, if the customer Robert Smith engages in a legitimate transaction of $10,000, an alert will trigger in accordance with U.S. laws. However, when the customer Bob Smith the money launderer subsequently withdraws $2,000 at each of his five accounts, will the bank's systems alert to the fact the accounts belong to a single entity and therefore may also require investigation?

Inability to Identify Hidden Relationships

According to a recent survey of banks, only 5% of respondents said their data provides their systems with insight and information on 100% of customer activities and relationships.
Source: CEB 2016 Financial Crimes Showcase Survey

Beyond simply standardizing and validating names and addresses, many solutions are incapable of identifying relationships between related third parties and expressing them as a visual. An institution needs to build a picture not only of its third parties, but also of other parties whom its third parties are doing business with. The use of graph databases enables companies to make sense of the masses of connected data and analyze the relationships between customers, products, places, and other entities. This is particularly important as companies seek to identify second and third level relationships that may not be readily apparent from data stored in traditional relational databases.

Sample graph database from the surveilLens solution



Big Data as a Third-Party Risk Management Strategy

Third party systems using some sort of automated technology are most certainly the clearest approach in minimizing third party risk.

> *In a recent survey, 51% of IT executives surveyed saw due diligence technology solutions as providing high value to their company.*
> *source: CEB 2016 Financial Crimes Showcase Survey*

Solutions powered by big data platforms such as the Apache Hadoop framework, that can integrate with existing applications and adapt to changes in regulatory and business demands in real time, however can exponentially enhance existing manual or even automated third-party programs. Such open sourced frameworks provide organizations with a means of identifying and aggregating data no matter where the data may reside or in what format it may exist, thus providing cost efficient compliance.

> *A recent survey found that just 8% of organizations surveyed used automated systems to manage the third-party risk management system while another 16% had implemented automated systems simply for screening and records management.*
> *source: 2016 Ethics and Compliance Third Party Risk Management Benchmark Report*

For a big data solution to provide value however it must be part of a formalized system that gathers and analyzes third party data. The beginning of the big data process lies in identification of relevant data for collection, sorting and analysis by the users who must make the decisions on the third parties. In order to make informed decisions, users must also be able to identify relevant data necessary for making their decisions, determine from where this data can be collected, how to collect the data, process it and present it in a manner that allows it to be used in a meaningful process.

Uses of Big Data Platforms in the Due Diligence Process

Third Party Onboarding

- Identification and collection of data from internal and external sources

Data Collection, Preparation, and Integration

- Normalize data and prepare staging for analysis

Presentation and Analysis of Third Party Data

- Development of risk assessment and profiles
- Monitoring of third party information to identify red flags
- Ad hoc analyses in real time to address questions and issues that arise

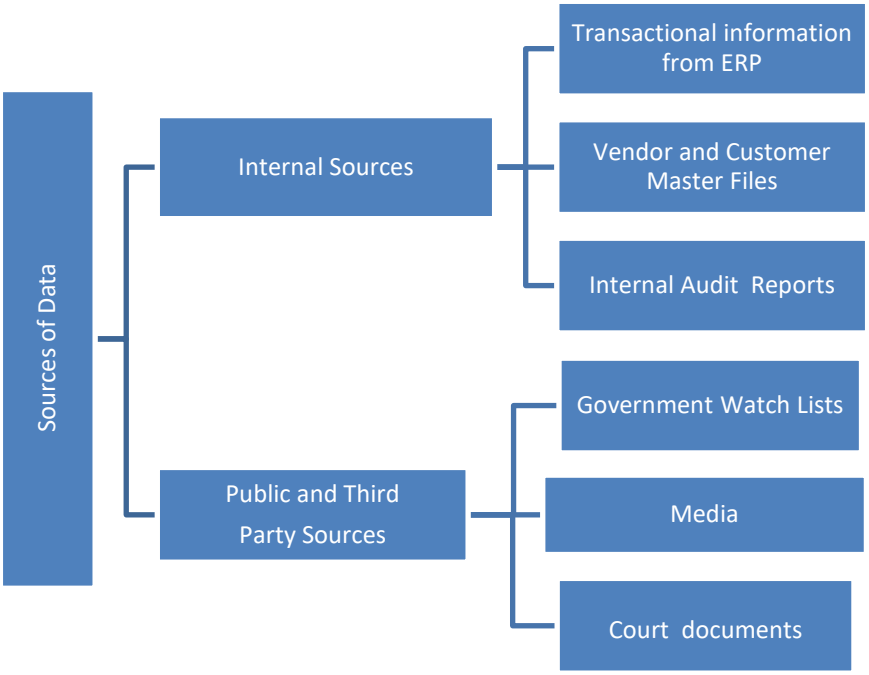
Reporting

- Development of new and emerging risks for internal and external constituents
- Delivery of prompt results enabling real time decision making

Using Big Data Technologies in the Third-Party Risk Program

Processing Large Amounts of Data in Real Time

Current legislation and best practices require the review of a wide variety of sources, (third party and internal) in multiple formats (structured and unstructured) in order to allow users to make informed decisions on third parties on a timely basis.



For example, using technologies such as natural language processing, combined with the power of machine learning (discussed below), big data platforms can perform comprehensive screenings against the ever-expanding number of watch lists as well as other data sources using the same cognitive processes as a human analyst without the time constraints associated with manual based research. Faster review and processing times facilitates the analysis, scoring, and aggregation of results for risk assessment purposes. Further, the platforms eliminate the need to hire additional people to accomplish the same review task.

Processing Disparate Forms of Data

Big data platforms allow compliance professionals to make decisions based on a complete set of data including legacy systems and applications that cause inconsistencies in third party data. Through the use of a central platform that combines structured and unstructured datasets, compliance personnel can analyze more variables simultaneously. This makes for more complete risk models and scoring and generates significant cost and time savings for by improving the velocity of decisions.

Advantage of Big Data Platforms in Third Party Risk Management

- Mine large volumes of historic and real-time data as it is produced.
- Allows organizations to rapidly bring together multiple data types for review.
- Identify potential adverse third-party relationships which may not be clear from a manual review.
- Creation of better risk models that provide broader and more comprehensive risk coverage.
- Detection of potential anomalies prior to internal or third-party review.
- Reduction of false positives allowing compliance to focus on actual third-party risk.
- Decreased compliance spend.

Machine Learning

Machine learning uses artificially intelligent computer systems to autonomously learn, predict, act and explain without being explicitly programmed. Simply put, machine learning eliminates the use of preprogrammed rule sets.

Big data platforms use machine learning to identify potential highlight trends and patterns that would otherwise remain invisible. Shining a spot light on these trends, creates questions and inquiries into how the business works which then allows the organization to predict and plan for previously unforeseen eventualities and disruptive events that would not have been identified by traditional means.

Reduction of False Positives

Most data is, by its very nature, dynamic. Standardization of data helps reduce false positives because it removes the need for inexact matching of data fields that can be better matched on an exact basis. IT-intensive standardization of data however introduces complexity and time lags into data preparation.

Big data platforms use a variety of techniques such as transliteration or transcription and variant matching logic to accurately identify similar data and to account for differences in cultures and geographies. For example, a third party based in the U.S. would spell the name Joseph differently than a third party in Eastern Europe (Josef) Middle East (Yusef). Accordingly, name and address standardization is of extreme importance when it comes to recognizing which details belong to the same entity and which denote separate ones altogether.

Identifying Relationships

Technologies such as link analysis can then be used to identify relationships between different datasets. Consider a third party ranked with a low risk score by the company's initial risk assessment. If, however, the third party in question is associated (e.g., a member of management) with another entity that had recently been the subject of a regulatory inquiry for corruption, the third party's risk score would need to be increased. Visual analytics can be particularly effective for linking structured and unstructured datasets and identifying indirect or second and third level relationships that involve several intermediaries. Running analytics on integrated datasets can therefore help companies isolate potentially risky relationships that would be difficult to uncover by studying scattered information independently.

Conclusion

Organizations should not seek to develop third party risk programs using a “one size fits all” approach. Every organization has its own unique mixture of policies, lines of business, business objectives, geographical locations, resources, and risk tolerance that will serve to lay the foundation for appropriately developed risk protocols.

In addition, each institution also has its own technology strategy and infrastructure. Having a platform that can integrate various data types and can identify a potential weakness or vulnerability based on the identification of patterns and trends can alleviate many of the limitations associated with traditional manual or simple automated diligence procedures.

However, while such systems should be considered as a key part of the organization’s broader third-party risk management process, the organization must understand they should serve to enhance the overall third-party risk management process. Organizations must also take steps to ensure that the existence of an overall program that is manageable, consistent, documented with the ability to respond to issues when they arise.

The SurveilLens Platform

surveilLens™ is a cloud based single technology platform that goes beyond systems to integrate into one solution, the elements of an anti-fraud compliance program with machine learning and the features of Big Data platform described in this document.

The surveilLens™ solution consists of several modules including: transaction monitoring, anomaly detection, case management, third-party due diligence policies and procedures, training and certifications, risk assessments, and internal controls. These modules work in isolation or with each other to create integrated workflows.

The various workflows can be customized and designed to give maximum flexibility and efficiency. The solution addresses organization, entity, industry, and region-specific requirements. It is a simple to use, plug-and-play model. Clients can pick as many modules as they need to develop or integrate into their existing compliance programs.

The surveilLens third party platform assists in client onboarding and KYC solutions for organizations in all industries and subject to varying regulations including but not limited to general fraud, anti-money laundering, and anti-bribery and anti-corruption compliance. The surveilLens solution provides comprehensive and in-depth global due diligence information on companies and individuals alike.

surveilLens utilizes the latest big data methods and artificial learning (AI) capabilities to monitor all of an institution's data including:

- ✓ *Processing of 10,000,000 + transactions a day (easily scalable beyond that)*
- ✓ *Up to 10,000 customizable rules*
- ✓ *100 percent data coverage and analysis*
- ✓ *Real time updates*
- ✓ *Capable of integrating data from multiple systems*
- ✓ *Dynamic rules based engine*
- ✓ *Database searching and matching*
- ✓ *Real time updates*
- ✓ *Anomaly detection*
- ✓ *Text mining*
- ✓ *Predictive modelling*
- ✓ *Advanced statistical analysis including machine learning*
- ✓ *Network analytics*

surveilLens™ is dynamic with self-learning capabilities. Designed to be implemented within a network or in the cloud, the surveilLens™ solution meets the highest security standards including but not limited to, global data privacy requirements. Thus, clients and compliance professionals can rest assured that their data is secure.

About surveilLens

surveilLens™ is a compliance solutions company that provides advanced technology-enabled governance, compliance, and risk (GRC) solutions. Our software, is designed to identify, mitigate, and remediate organizational risks while bringing convenience, effectiveness, and efficiencies to an organization's overall compliance program. Founded by professionals with decades of experience in compliance, technology, data science and auditing, we offer our clients customized and scalable compliance solutions. Our goal is to transform the traditional approach to GRC from a manual process to an automated one, where all a company's data sources are harnessed to provide meaningful insights.

For more information:

SurveilLens

30 Wall Street, 8th floor
New York, NY 10005
(212) 804-5734

201, 2nd Floor, 18/1, Sufiya Elite,
Cunnigham Road, Bangalore
560052, Karnataka
India

Visit: www.surveil-lens.com
inquiries@surveil-lens.com