THE DEFINITIVE GUIDE TO DUE DILIGENCE AUTOMATION

6 CRITICAL STEPS TO TRANSFORMING YOUR DUE DILIGENCE PROCESS

Sara Shah, Esq., Associate General Counsel & Senior Compliance Consultant, GAN Integrity

GAN
INTEGRITY

TABLE OF CONTENTS

INTRODUCTION

There are many functions of a Compliance Manager's job that necessitate due diligence, but, in today's globalized economy, we recognize that the most important purpose of due diligence is in complying with the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act. Under both the FCPA and the Bribery Act, rogue third parties represent the single greatest risk to a company. In fact, the vast majority of FCPA cases involve conduct by third parties.

We cannot emphasize the importance of complying with these Acts enough; over the past eight years, companies from around the world have landed themselves on the FCPA Blog's "Top Ten List" of enforcement actions, and there is no sign that the pace of enforcement will abate anytime in the near future. Just a few months ago, we saw 2016 kick off with VimpelCom's $795 million resolution with US and Dutch authorities.

This increased scrutiny has placed more emphasis on an already difficult job. While compliance programs are under the microscope more than ever, guidance around how to properly construct and operate third party management systems that hold up to this scrutiny has been thin. In their current states, most systems are inefficient and riddled with errors, each one carrying its own risk potential.

It doesn't have to be this way.

The good news for you, the Compliance Manager, is that there is a better approach. We have identified six crucial steps to help you establish a more systematic approach to managing third-party risk; a blueprint for transforming your existing due diligence practices into a streamlined and automated due diligence system. These steps will give you visibility and control over your entire due diligence framework, which, in turn, will mitigate risk to you and your organization.

STEP 1: CAPTURE KEY DATA AND AUTHORIZE IT

Good data is the foundation of proper due diligence. If your data is flawed, your due diligence data will be fraught with duplicates and holes, thus nullifying – or at least severely impairing – the results of the entire process. It’s an unfortunate reality that, due to the prevalence of siloed data and the use of manual processes in spreadsheets, this is a situation most Compliance Managers face on a regular basis. You need to collect key organizational information on the entity and the department that initiates due diligence into a centralized third party management system. While the upfront effort you expend on this task may seem cumbersome at first, you’ll be setting yourself up for a much smoother compliance ride down the road if you take the time to do it. To this end, creating automatic alerts is a key time-saving and organizational feature of successful data aggregation – use your own tools or a third party!

> If you capture your key data correctly, you’ll not only fill in your compliance data holes; you’ll be able to identify and mitigate risks before they become a problem.

STEP 2: INTERNALLY ASSESS THIRD-PARTY RISK

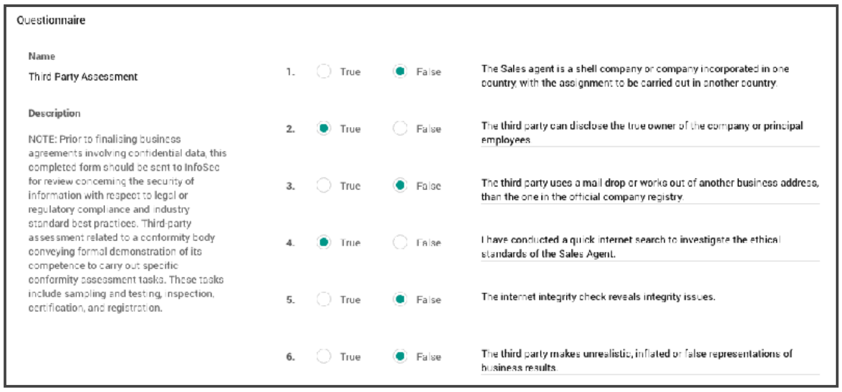
After all of your data has been authorized, the initial risk of the relationship between the company and a third party should be evaluated by asking the entity or department initiating the business a number of relationship questions via a questionnaire.

This might include topics such as:

- Previous experience with the third party;
- Purpose of the business relationship;
- Interaction with the government officials;
- Description of activities performed by the third party;
- A country risk rating using the TI/CPI index;
- Type of compensation; and/or
- Danger signs concerning payment terms.

> Including a set of "red flag" questions ensures the risk questionnaire can be used to create guidelines for the depth of an investigation that will be conducted on a third party, and will determine the initial risk level of a specific third party to an organization.

You can automate sending risk questionnaires to the entity or department(s) initiating the business relationship ("Originator"), which contain sets of "red flag" questions that will trigger requests for additional information. Questionnaires with the Originator's responses should be recorded in a centralized system and the team conducting the due diligence should be notified automatically via email upon its completion.



Questionnaire

Name

Third Party Assessment

Description

NOTE: Prior to finalising business agreements involving confidential data, this completed form should be sent to InfoSec for review concerning the security of information with respect to legal or regulatory compliance and industry standard best practices. Third-party assessment related to a conformity body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. These tasks include sampling and testing, inspection, certification, and registration.

1. ○ True ● False The Sales agent is a shell company or company incorporated in one country, with the assignment to be carried out in another country.
2. ● True ○ False The third party can disclose the true owner of the company or principal employees
3. ○ True ● False The third party uses a mail drop or works out of another business address, than the one in the official company registry.
4. ● True ○ False I have conducted a quick internet search to investigate the ethical standards of the Sales Agent.
5. ○ True ● False The internet integrity check reveals integrity issues.
6. ○ True ● False The third party makes unrealistic, inflated or false representations of business results.

Note on the Timing of Background Screenings

Typical due diligence/compliance processes include conducting background screenings on potential third parties after risk assessments are conducted. This often results in incomplete data and almost always creates inefficiencies. To correct this (according to forthcoming ISO guidelines and global best practices), **this step should be a part of the risk assessment process itself.**

Think about it: Shouldn't factors such as if a third party has been involved in criminal investigations, sanctions or litigation be a part of determining their risk score? What about whether if a party is, or has connections with, a government official?

At this stage, a third party should be vetted against an internet database or against other available sources (sanctioned party lists, PEP, etc.) with analyst reviews for false positives. This gives an accurate determination of which questionnaire should be completed rather than relying on a risk score calculated based solely on the responses of the Originator, who may likely have a vested interest in obtaining the least amount of information.

STEP 3: CONDUCT EXTERNAL DUE DILIGENCE

This critical step allows a business to establish a holistic and neutral picture of a third party and ascertain whether a company should establish a business relationship with a partner by having them complete an external questionnaire.

Due diligence questionnaires are modified, redacted or augmented according the risk levels derived during your risk assessment.

Conducting external due diligence is easily the most complicated step of this process, so we've broken it down into action items. Note that background checks and external questionnaires are interchangable items depending on your workflow.

Background check: Upon receipt of the internal questionnaire, a thorough background check should be conducted on the third party. This includes, among other things:

- Searching internet databases
- Screening against government, regulatory or disciplinary lists
- Conducting adverse media searches
- Discounting Politically Exposed Persons (PEPs)

> It's crucial to document background check findings for evidential purposes. An internal or third-party management solution can help you update your system of record automatically, saving time.

Risk score calculation: At this point, a risk score must be calculated based on the Originator's responses as well as the results of the background screening. The score will determine the risk level of a business relationship to be Low, Medium or High risk. The risk score of a third party determines the minimum required scope of due diligence that must be conducted through a set of questions in the due diligence questionnaire. In general, the higher the risk level, the deeper the investigation that must be conducted. This ensures that the approval process, subsequent to this phase, is based upon sufficient information. The risk score will, in turn, determine the corresponding approval process.

External due diligence questionnaire: Assign and send an external questionnaire to the third party. In the questionnaire, the third party will be asked to confirm or provide more information about its business activities. It should include information that may have previously kept on file as well as external information that was obtained from independent sources. As previously stated, the level of questioning will be determined by the Originator's responses and the results of the background check.

A standard high-risk questionnaire typically includes the following:

1. The third party's basic information and qualifications (e.g. upload of business licenses, ownership, type, history and infrastructure of the third party);
2. Checks of third party's key persons against an internet database or against other available sources (sanctioned party lists, PEP, etc.) with analyst review for false positives;
3. Terms and conditions of the proposed business relationship;
4. Bank details and bank references;
5. Connections with government officials;
6. Current and previous litigation, criminal investigations and sanctions involving similar activities to be performed by the third party;
7. Contact information for business references; and/or
8. Information to be collected from external reliable sources (e.g. financial reports, commercial registry).
9. Relevant requests for documentation

Sending external questionnaires and tracking their completion progress can get very complex, very quickly. It's highly recommended that you implement some sort of automation for questionnaire assignment and distribution that can be tied to your risk score calculations.

STEP 4: SUBMIT THE DUE DILIGENCE QUESTIONNAIRE FOR REVIEW

Once the third party has completed the due diligence questionnaire, adjust your risk score to accommodate for their responses. Then, a compliance reviewer must make the determination of whether the third party will be approved or rejected after review is complete.

Note: Often, the employee championing a partnership with a third party has an interest in hiring them. They should not *be the only reviewer, nor should they be the final decision-maker determining the relationship.*

1. Once the Originator has completed the due diligence questionnaire, the form should be submitted for compliance review–ideally through a platform or system that allows those in control to track its submission and status in the review process.
2. The third party should automatically be added to a queue for review to the compliance office and an email notification must be sent to the approver in the compliance office.
3. Document all movement on the submission for future audits and reporting purposes. This can be done manually, or automatically if software has been implemented.

STEP 5: APPROVE (OR REJECT)

Make a determination and notify the Originator on whether the business will transact with a specific third party. To do this efficiently, you can use the following process:

1. Set up selected approvers to receive automatic email notifications to review the assigned due diligence questionnaires.
2. After reviewing the information provided directly in the due diligence questionnaire and risk assessment (ideally at the same time), the respective approver needs to decide whether the third party is acceptable or whether there are any objections to due diligence. A compliance reviewer may have questions or require additional clarity on some of the responses. If so, the approver can send the due diligence questionnaire back to the Originator, the third party or to previous approvers for clarification.
3. The approver will either approve or reject the third party and will submit their determination through a centralized system or software platform.
4. Once this has been decided, the system should automatically notify the Originator of the results via email, which includes the determination, the reasoning for the decision and all supporting documentation—saving it for historical reference.

STEP 6: FINALIZE: POST-APPROVAL PHASE & CONTRACT

At this phase, if the third party is approved, the business can now proceed to establish a relationship with them.

1. After the final approval of the due diligence process, a business relationship with the third party can now be established.
2. As additional information on the transaction or contractual details become available, they should be registered and stored alongside the rest of the partner's due diligence information.
3. Based on their respective risk level, the third party is automatically scheduled for recertification at predefined intervals. For instance, a business may wish to recertify high risk third parties every year, medium risk every two years, and low risk every three years. If they are sanctioned, they should be put up for review immediately.
4. This can be accomplished through automated recertification reminders, which are essential to this portion of the process. They serve to reduce errors and increase efficiency over time.
5. The partner may be required to sign policies and complete trainings once approved. Ideally, once a business relationship has been established, these activities will have notifications and/or materials associated with them that are automatically sent once the company has been marked as a business relationship.

Having most new partners complete trainings and sign documents is defined as a best practice, but at a minimum it should always be done with high risk partners.

YOUR NEXT STEPS

We hope this guide has given you some practical ways to begin implementing some great best practices in your due diligence process. Our goal is to simplify and enhance your daily work through automation; we want your life to be as stress-free as it can get.

While the entire process described in this whitepaper can be done by hand, the value of using automation to comply with FCPA regulations is clear. Currently, the world's top companies are using GAN's all-in-one software to transform the way they handle due diligence – saving time and reducing risk. We invite you to try it out for yourself: **Free for 30 days with less than 24 hours of ramp-up time**.

Hello! Effortless Compliance.

GAN'S ALL-IN-ONE COMPLIANCE MANAGEMENT SOFTWARE.

...brings your critical compliance systems, docs and data together into one powerful, integrated system.

Request Demo

Learn More

MONITORING & REPORTING

Track, monitor and report your compliance status, data and results in a single place.

RISK ASSESSMENT

Create risk reports and implement mitigation activities through a global risk catalogue and local manager inputs.

POLICY

Manage your policies: Develop, publish and assign policies to employee groups for signing. Track and report completion rates.

TRAINING

Train employee groups with e-learning courses and tests. Assign to your employee groups. Track and report the results.

DUE DILIGENCE

Evaluate, track and store third party and employee due diligence. automatically.

GIFTS & ENTERTAINMENT

Register gifts. Upload documentation. Review, approve, or reject requests. And, monitor and report.

INVESTIGATIONS

Automatically create new cases, manage tasks and report results with ease. Always keep stakeholders in the loop.

MANAGEMENT

Assign, coordinate, and manage compliance initiatives with employees, business partners, HR, Finance, and more.

The world's top companies are using GAN's all-in-one software to transform the way their compliance programs operate.

IPSEN Innovation for patient care · SGS · Vestas · HEXAGON COMPOSITES · JCDecaux · NIBE

SKF · TORM · ELTEL · JX · sobi

Share this Ebook!

GAN INTEGRITY