Framework for a Third Party Risk Management Program

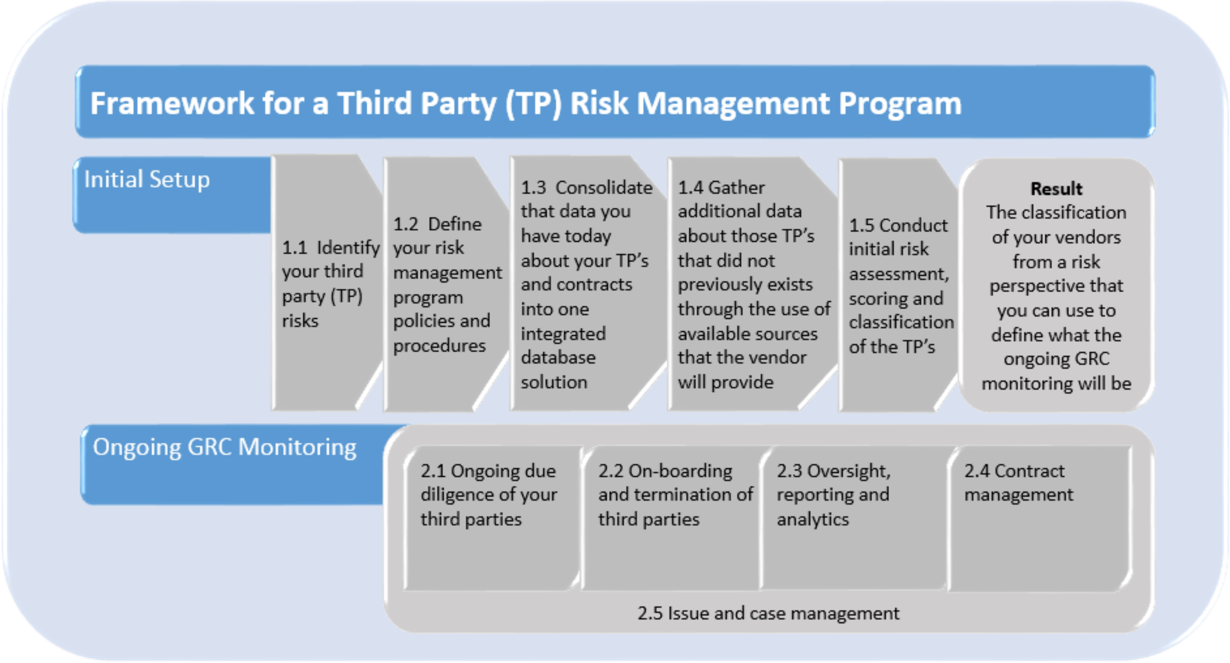
Get a clearer picture of the risks posed by vendors and third parties

Framework for a Third Party Risk Management Program

In this paper we outline the key steps that you will need to take when constructing your requirements for a modern and dynamic third party risk management solution. A proposed framework to implement your program is presented for your review.

When designing a third party risk management program, it is proposed to divide the process into two distinct stages:

1. Initial setup of the Third Party Risk Management program
2. The ongoing monitoring of the Third Party Risk Management program



Framework for a Third Party (TP) Risk Management Program

Initial Setup

1.1 Identify your third party (TP) risks

1.2 Define your risk management program policies and procedures

1.3 Consolidate that data you have today about your TP's and contracts into one integrated database solution

1.4 Gather additional data about those TP's that did not previously exists through the use of available sources that the vendor will provide

1.5 Conduct initial risk assessment, scoring and classification of the TP's

Result
The classification of your vendors from a risk perspective that you can use to define what the ongoing GRC monitoring will be

Ongoing GRC Monitoring

2.1 Ongoing due diligence of your third parties

2.2 On-boarding and termination of third parties

2.3 Oversight, reporting and analytics

2.4 Contract management

2.5 Issue and case management

Initial setup

The initial setup of the program is focused on:

1.1 Identifying the risks created by your firm’s use of third parties
1.2 Defining your policies and procedures for monitoring third parties
1.3 Consolidating your existing third party profile data and contracts into a single data repository
1.4 Closing critical gaps on missing data on your third parties
1.5 Conducting an initial risk assessment

The initial setup should also consider: (a) the due diligence processes to be undertaken based on the risk classification, (b) the approval and review processes and (c) the implementation of processes to capture and manage any issues.

1.1 Identifying the risks created by your firm’s use of by your third parties

Identifying and defining the risks represented by your third parties is the first step in your third party risk management program. This process should involve identifying the scope of your risk management program including the risks you should be monitoring and the types of third party you should be assessing.

1.2 Define your policies and procedures for monitoring third parties

The first step with any monitoring program is likely to be an updated definition of your policies and procedures and to obtain all internal approvals. These policies and procedures at a minimum need to include the following:

- Roles and responsibilities
- Risk assessment process
- Due diligence in selecting a third party
- Ongoing monitoring
- Third party onboarding
- Third party termination
- Oversight and escalation

1.3 Consolidate your existing internal third party profile data and contracts into a single data repository

One of the principal challenges initiating the process to more effectively manage your third parties is the probable dispersion of third party data across the firm. This is exacerbated if there are multiple divisions, departments, countries and if they are stored in multiple data repositories. For effective program management, these sources all need to be assembled into a single integrated operating platform to enable you manage your program effectively. Although you can aggregate the existing internal third party data manually, you should consider how a third party vendor risk management solution may be able to help with aggregating the data:

- Does the solution enable you to easily capture the data elements from existing data sources?
- Does the functionality of the system have the capability for effective workflow processes to capture the data from internal sources e.g. questionnaires, data entry forms and data entered by the third party itself?
- Does the solution allow for the capture of data through integrated feeds from existing external data e.g. third party files on your internal databases, to ensure an easier and more precise transfer from existing systems to your new system?
- How flexible are those capabilities at meeting the needs of your data gathering exercise?
- Can the data you have aggregated about the third parties be easily queried, filtered and reported on?

1.4 Closing critical gaps on missing data on your third parties

It is highly probable that you will not have all the data you need from internal sources to conduct your risk assessment on the third parties. You will need to be sure that your platform is capable of gathering data from multiple external data sources.

The external data you need can come from either (a) generic external data sources e.g. company, market data, news items (b) from the third parties themselves or (c) potentially internal employees that have relationships with the third parties. You will need a system that has the ability to capture data for the following:

- Integrated data interfaces from trusted external sources. These include feeds from firms like Thomson Reuters, Standard & Poor's and Dun & Bradstreet. These feeds allow you to automatically run checks on any third party or business partner and ideally they should be integrated into the system and run off the same platform.
- Questionnaires completed internally by relationship managers or other internal staff that have insights on the third parties being monitored.
- Questionnaires and profile data completed by the third party themselves.

The ability to push out information requests to third parties is an essential element in a dynamic vendor risk management solution. It should have very good questionnaire functionality (Think SurveyMonkey® on steroids) and have features for assurance of completion! The better this type of functionality is, the more efficient your data gathering process will be.

1.5 Conducting an initial risk assessment including risk scoring and risk classification

Once you have your initial data about the third party, it is time to assess the risk and assign a risk classification to each vendor or third party. You will need to be methodological in your approach as regulators are expecting to see a robust, well designed structure. A risk assessment can be conducted in many ways including manual classification with documentation on why you have taken a particular risk view, to questionnaires to third parties with scoring, to more robust scoring using a risk matrix with a weighting of factors.

Risk assessment is different for every business but there are some fundamentals that apply to all organizations. Typically, you will be monitoring for larger red flag issues. While this may differ by industry, your common sense assessment will generally include the following:

- Type of service being provided
- Access to internal data involved in providing the service
- Nature of data set involved (client confidential, private data, financial transactions, identifiers, passwords, etc.)
- Data and information security expectations (related to nature of data)
- Financial standing of the vendor
- The size of the contract
- History of the relationship
- Identifying the beneficial owners of the third party business
- Location (country or region) where services are provided from or where the firm is headquartered. Some jurisdictions have looser regulations, a noted tendency to corruption in the market, opaque business practices or a lack of enforcement of good corporate governance
- The strategic importance of the third party to your business or service proposition

Risk scoring is the process of giving a value to the level of risk a third party represents. The total risk score is built on multiple values. Depending on your model, the structure and content of the total score may be a complex process but it is essential if you are to deliver an accurate assessment that will protect the organization. The MCO solution delivers the risk score through our Risk Transparency Matrix (patent pending) which allows an organization to evaluate a vendor on anywhere between 1 to 10,000 data points!

This initial risk classification will typically deliver a small number of levels of assessment of the third party such as low, medium and high. Others segment into low, medium, high and critical classifications. The solution should be able to grow as often you will want more sensitive classifications as the of the third party risk management program matures. The initial classification during the setup process would typically determine the degree of ongoing due diligence and monitoring within the program. Higher risk classifications may also initiate a deep dive assessment of the vendor.

Once you have assessed, scored and classified your third parties, you will then want to implement your ongoing due diligence and monitoring processes.

Ongoing Third Party Program Monitoring

Once the program has been set up, the challenge now is to operate the ongoing monitoring of your third parties. These activities include the ongoing due diligence of existing third parties, the on-boarding and termination of third parties, contract management, issue management, reporting and oversight.

2.1 Ongoing due diligence of your third parties

This part of the process requires deeper dives into areas of risk such as IT security, financial stability, corruption and bribery etc. This is accomplished through multiple activities including the use of in-depth questionnaires, the screening of third parties against external databases such as World-Check, Dun and Bradstreet for financial standing and the scheduling and documenting of activities such as on-site visits, phone interviews and so forth.

It is estimated that 90% of the risk management team's time will be spent on activities around existing vendors and third parties. This on-going due diligence is essential to the success of the program and an area where automation can make a significant contribution.

The priority is to execute your defined monitoring program to protect against reputational and regulatory risk. Any vendors or business partners who are classified as high risk must be monitored more closely and an automated system allows you to do this efficiently.

Now that your ongoing due diligence program is active, you can start to look at specific tasks such as certifications and attestations to ensure your policies are being followed through by all parties.

2.2 Onboarding and termination of third parties

On-boarding of new third parties is a key process for the firm and implementing procedures to ensure that the correct third parties are on-boarded is critical. It is an important part of your third party risk management program. It needs to be implemented consistently across the organization and this consistency is key to the long term evolution of your program.

Termination of the relationship with a third party is also very important and is often a focus for regulators. There are business processes focused on the addition of new vendors but the processes on termination often receive much less attention. Firms should have processes in place to identify when and how third parties should be terminated and to ensure completion of the procedures associated with the proper termination of the relationship. Again, to ensure consistency, these processes should be automated across the organization.

2.3 Oversight, reporting and analytics

Once your third party risk management program is up and running, oversight of the program and the ability to conduct analytics of the program is very important. An automated solution should enable firms to quickly see the risk classifications of their third parties, the risk assessment and due diligence activities that are upcoming and past due. Alerts that have been generated and any cases or issues raised within the program, and their status, should all be available at a glance. The ability to conduct analysis on the risks presented by the third parties and delve into the source of the risks through visual tools such as matrices is key. Other analytical reports that show changes in risk profile over time are also very helpful to show trends.

2.4 Contract management

So now you have an efficient third party risk management process in place. Great, but what about the contracts? At the end of the day, the contract is the document everyone will revert to if there is an issues as it contains all the important details of the relationship and defines the terms of engagement. And, we must also recognize that they are especially important at the end of the relationship when two parties need to extricate themselves from each other.

In terms of technology, contract management is not all that complicated. The critical functionality begins with ensuring you have the contracts stored centrally with key data elements (metadata) identified per contract. Examples of important metadata are effective date, term, jurisdiction, cancellation periods, auto-renewal clauses, indemnity, and confidentiality clauses. The key attributes of each contract need to be closely monitored and managed, and a technology solution will really assist in monitoring this contractual risk with third parties.

2.5 Issue and case management

When you are classifying the risks and conducting due diligence you also need a robust system that can manage those occasions when a supplier or third party does not meet the standards set out in your policy documents.

The majority of third party risk management systems are dealing with thousands of partners on a regular basis and need to process a very large volume of data related to their interactions with and on behalf of the organization.

When you establish your program, you will write the rules for engagement with all external partners and suppliers. These rules are intended to bring your policy to life and ensure you meet your regulatory responsibilities, so it is critically important to success that all partners understand and meet them throughout their engagement with the organization.

You will need a robust case management solution to manage all the cases and issues related to each third party. The software will translate policy into rules and each rule will have limits, threshold values or triggers associated with them. The system must be capable of identifying the vendor or third party whose profile, circumstances, activities and other actions are not in keeping with your program rules.

Once a rule is broken or a potential match with a name on a screening check is found, an alert should be generated. Robust systems will help you manage these alerts by creating automatic workflows and routing the alert for review to defined personnel in the organization.

Alerts can then be reviewed by the responsible individuals and if they require further investigation a case can be created.

Cases can be assigned to an owner and should have the capacity to have multiple individuals associated with them, with privileges to add comments or documents as well as being able to resolve and close the case where appropriate. Cases may need to be routed through multiple people on the journey to resolution and close, and have due dates associated with their resolution.

Once a system is up and running and data begins to flow, your rules will be constantly running, checking and verifying data from all third parties. There is a certain peace of mind and confidence that comes from the 'always-on' functionality of an automated third party vendor risk management solution.

Summary

In summary, implementing a third party risk management program is key to managing the increasing risks represented by third parties. However, there are various components that need to be considered when implementing a third party risk management program. Managing all of these complexities requires the implementation of an automated risk management solution that can handle the:

- Aggregation of all third parties in one central location
- Augmentation of data about third parties from external sources
- Assembly of third party data using questionnaires and other data gathering techniques
- Classification of third parties based on risk
- Ongoing third party due diligence effectively
- Remediation and resolution of issues that arise
- Provision of robust reporting and analytics on the entire program

All of the above needs to be conducted on a system that provides full audit and transparency for auditors and regulators.

More Information

To make contact and arrange a call with one of the MCO team, click here or call 1-866-951-2280
To keep up to date with news and information in this area, subscribe to our blog here or visit *www.mycomplianceoffice.com*

Our integrated software solutions give you a clearer picture of the risks posed by vendors and third parties. Our unique Risk Transparency Matrix will harvest from 10 to 10,000 data points on every third party, giving you exceptional oversight and control.