Διαχείριση ρίσκου 3ων μερών, στο COVID-19 πλαίσιο αυξημένης «επαγρύπνησης»

Σοφοκλής Καραπιδάκης, Διευθυντής Κανονιστικής Συμμόρφωσης και Υπεύθυνος Προστασίας Δεδομένων, ΜΥΤΙΛΗΝΑΙΟΣ

PRESENTATION

AGENDA

1. Starting point
2. 3rd Party **definition** for the purposes of the **sanction screening**
3. 3rd Party definition for the purposes of the **integrity due diligence**
4. Compliance **red flags**
5. Highlights **during** COVID 19 lock down
6. Highlights **after** COVID 19 lock down

Starting point

- Organizations employ and cooperate with 3rd parties through their value chain either with: a. customers, b. suppliers c. joint venture/ consortium partners (a.k.a. business partners)
- In some cases organizations may **become liable for actions of their business partners** and their cooperation with them as they act not only in the Organization's interest/favor but also represent them.
- **Compliance due diligence and sanction screening** is the core basis to identify the compliance exposure 3rd parties create for the organization in the fields of **corruption, fraud, money laundering, conflicts of interest, existence of a politically exposed person, ultimate beneficiary ownership and sanction prohibition evading**.
- Not all risks apply to all business partner relationships therefore there is a need for **business partner classification** versus horizontal measures that would create noise and distract the organizational resources. As of that a risk-based approach is recommended.
- It is the responsibility of all first line representation to be involved in the business partner onboarding assessment and afterwards in the monitoring process under the guidance of Compliance.
- Management needs to make **risk informed decisions**, thus a proper analysis of the applicable risk for the organization needs to take place beforehand.

3rd Party definition for the purposes of the sanction screening

Sanctions risk (risk to engage with an entity (individual / legal person / vessel) that is financially restricted due to violation of human rights, terrorism, human trafficking, money laundering or affiliation with other sanctioned persons)

The applicable sanction lists for every organization are resulted from the Compliance Risk assessment that is conducted and are based on the countries of operation and representations made to other organizations (e.g. financial institutions, suppliers or customers). Typical sanction lists for a European organization are:

- United Nation Security Council consolidated sanction list
- European Commission Financial sanction list
- Office of Foreign Asset Control (OFAC) programs by the US Department of Treasury that includes territorial and sectorial and secondary sanctions
- HM Treasury - Office of Financial Sanctions Implementation HM Treasury (OFSI) list (UK)

The organization needs to ensure that it screens **all 3rd parties** against the applicable sanction lists during onboarding and afterwards in frequent intervals.

Sanction screening is mainly being conducted through name screening against current sanction lists either in an automated or manual way

In cases of increased risk (country sanction risk, sectorial risk, red flags, major cooperation), an **enhanced due diligence** is being performed which identifies in depth the ownership structure (ultimate beneficiaries) and the control of each organization, the sanction screening matches for them and whether the business operations of this 3rd party comply with the organization's policies.

3rd Party definition for the purposes of the integrity due diligence

Corruption risk (risk to engage in cooperation with an organization or physical person that either has history on bribery or corruption or its setup created various question marks and lack of transparency)

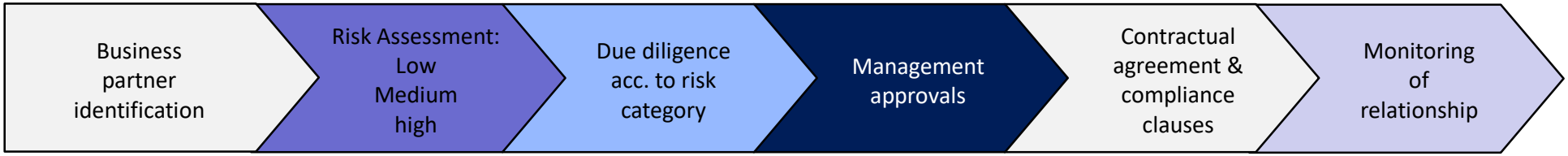
This risk applies mainly in business relationships of increased corruption risk that are the representation of an organization with the ability to influence decisions or the business conduct. Examples are sales consultancy, business representation, lobbying activities, intermediary activities (licensing, obtaining permits, tax or custom intermediation), resellers and distributors.

Joint venture and consortium partners need also to go through the compliance due diligence since they also entail a risk for the organization

The organization needs to ensure that it conducts the appropriate compliance due diligence for the above categories of agreements using a risk-based approach to first classify the business relationships for the in-scope 3rd parties and then apply the appropriate depth of due diligence.

.

3rd Party definition for the purposes of the integrity due diligence



Factors considered during the risk assessment

- Country of 3rd party establishment/ operations/ agreement performance
- Type of relationship
- Government connections relevant to the agreement
- Association with the end party
- Compliance red flags (adverse press findings, unusual behavior, lack of business rational etc.
- There is no monetary threshold that defines risk

- ❑ Due Diligence is performed by the employee in contact with 3rd party with the help of the 3rd party to provide documentation/ information and is checked and enhanced by Compliance.
- ❑ Due diligence activities are **scaled to the level of exposure**. Compliance aspects are considered to the appropriate risk category depth varying from fact findings to business plausibility checks and business references. This is not a check the box exercise.
- ❑ The outcome of the due diligence is the risk level and type posed by the specific 3rd party relationship to the organization.

- ❑ Management shall make afterwards a **risk informed business decision** and apply mitigation measures where applicable

- ❑ All employees involved in the 3rd party relationship shall escalate any red flag during their cooperation with the 3rd party and reassess the relationship.

Compliance red flags for 3rd parties (business partners)

Red flags are circumstances that may indicate a risk in regards to the integrity of the business partner. They can happen anytime, before or during the contractual relationship and need to be taken seriously.

Examples:

- BP has **bad reputation** for corrupt activities (from well-sourced internet or press articles)
- BP insists on **anonymity** (ecommerce, no written communication)
- BP **lacks skills, resources** or track record to perform the contractual services (and further subcontracts all of the contract)
- BP uses **unusual methods of payment** (uses intermediaries, 3rd party accounts, promotes reasons for cash payments, split payments etc.)
- BP contract and/or **invoices lack detail** or description does not match services
- BP has close **ties to Government Official** who is in position to influence decisions in favor of the organization or a PEP has ownership rights over the BP.
- BP is **uncooperative to provide requested information** (e.g. audit related information, ownership structure, company registry)
- There is **no obvious reason** for the use of the BP, and the organization could conclude the project w.o. the BP.
- Need for BP engagement arises **just before the contract is awarded**
- BP requests additional entities to be included in the payment that are not stated on the contract/agreement
- BP is a **new entity** with less than a year business activity thus with no documented financial records
- BP provides **offshore bank account** (or owned Shell company account to get paid)
- BP denies provision of personal ID documentation (passport/ National ID)

Highlights during COVID 19 lock down

During COVID 19 lock down:

- Temptation to think that normal rules do not apply. The categorization between **essential and no essential** services should not exclude compliance from the essential services since the law is always valid.
- Alert the employees for compliance **red flags** and readjust to accommodate current environment.
- Ensure **access to all tools** necessary for due diligence and sanction screening
- Ensure that Compliance team members are operational and apply no compromise policy
- Ensure that high risk 3rd parties continue to have the necessary resources to perform their tasks
- Be prepared for **new 3rd parties in short notice** due to existing 3rd party inability to fulfil their obligations or the appearance of new business models to accommodate the new environment. Proactively consider how the crisis may consider current risk exposure and identify potential bottlenecks with the help of the business.
- Ensure that all 3rt party **subcontracting activities** are performed by the 3rd party with the appropriate diligence
- Replace physical **educational courses** with digital ones.
- Make the Compliance resources **easily accessible** and available to 1st line of defense
- **Be alerted** as fraudsters usually thrive during unexpected situations

Highlights after COVID 19 lock down

- Governments are already designing the business activities after the lockdown and it is predicted that there shall be an increased flow of money to investments and business activities in a rapidly increasing way in order to bring back on track the global supply chains.
- **New operational and business models** that were not well exploited before are getting ground and may result to unidentified compliance risks.
- **Increased Government participation** in affected organizations through state support shall create the need for a robust due diligence and a critical eye on the new or continuing 3rd party relations
- **Vertical integrations** in the weak value chains shall raise risks such as antitrust and corruption.
- Have in mind that the value brought by in person contacts and on site visits can not be replaced by video calls and virtual meetings in which the compliance officer is able to recognize and feel the red flags.

THANK YOU

Sofoklis Karapidakis

Compliance Director/ DPO

mytilineos.gr