“End to end Compliance 3rd party due diligence with the use of a software tool”

Sofoklis Karapidakis, Compliance Director and Data Protection Officer, MYTILINEOS S.A.

PRESENTATION

AGENDA

1. The compliance need/ business case
2. Commonly applied standards
3. The solution
4. Benefits

The compliance need/ business case

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 many cases organizations may **become liable for their business partners actions** especially when the latter act as intermediaries or represent the organization.

Compliance due diligence is the core basis to identify the compliance exposure that 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 the same risk applies 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 the first line of defense 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.

Commonly applied standards

rrently compliance due diligence is usually being conducted through:

various standard collection forms e.g. KYC, other questionnaires sent to the business partner to fill in

Background searches through various publicly available information e.g. local registries, annual reports, web searches.

Background searches using dedicated databases for adverse findings, sanction screenings, PEPs, UBOs

email inquiries for additional documentation (e.g. registration documents, certificates, internal policies) and clarificatio
mostly when adverse findings are spotted.

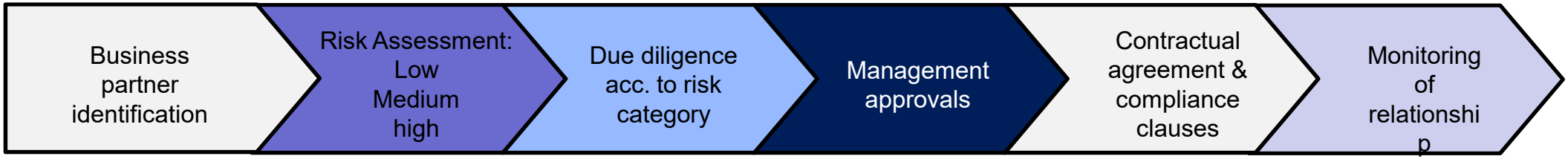
Most methodologies do not differentiate acc. to the risk each relationship entails for the organization, resulting to most
he times unnecessary effort and burden for all involved stakeholders.

All communication and files are usually stored either on inboxes or drives in various formats in a **poorly organized form**
and the due diligence is difficult to be reproduced.

Most of the times various stakeholders are involved each in different stage of the due diligence making the **information flo**
difficult to be traced.

The solution

Software application hosted in the organizations intranet that supports Interaction between the necessary stakeholders involved in the due diligence process under the discrete roles of originator, compliance and management.



Factors considered during the risk assessment (There is no monetary threshold that defines risk)

- Country of 3rd party establishment/ operations/ agreement performance re. corruption risk
- Type of proposed 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.

} Business partner risk category: High/ medium/ low

- ❑ Due Diligence is performed by the originator 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 for 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 compliance risk exposure 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.

Benefits

1. One place for all BP compliance due diligences with supporting documentation and decisions taken (Centralization)
2. Database with access rights ensuring that no information is lost due to employee changes (security, data retainment)
3. Easily reproduction of the due diligence and the circumstances under which decisions were made. (Clear audit trail)
4. Reusable information for future cooperation by same or other divisions (Reusability)
5. Seamless involvement of compliance and originator till highest due diligence quality is reached (Quality)
6. Management has all structured information and executive summaries to make an informed decision (risk-based conclusions)
7. Classification of BPs acc to their risk so that the necessary action and effort is then taken. Use of a calibrated algorithm that results to 3 risk categories. (Scalability)
8. Use of a comprehensive methodology so that the originator knows what is to be collected just after the risk classification. (Transparency)
9. Continuous monitoring of the BP through out its engagement (end to end solution)

THANK YOU

Sofoklis Karapidakis

Compliance Director/ DPO

mytilineos.gr