Third Party Risk Management (TPRM)

Netradyne Infosec Team

Significance of TPRM

Purpose

- To assess third-party vendor risks which potentially exposes Netradyne to any kind of attacks, data breaches, and reputational damage.
- This is particularly important for high-risk vendors who process PI / SI / customer data, or intellectual property
- As vendors have access to our PII/sensitive data, it's our responsibility to safeguard our data

Benefit

- This can support us proactively to assess the risk before arriving the decision of engaging vendors and monitoring
- To identify any issues that warrant a restructuring of the deal
- Ability to surface third-party risks before it’s too late to remediate
- Allow for the identification and quantification of a vendor’s Infosec posture

Outcome

- This will mature in safeguarding the organization from all types of risk
- This will enable us to meet regulatory requirement as data controller and data processor
- Understand the threat landscape and identify common threats

Potential Risks Involved with Third Party

.

Technology Risk
Operational Risk
Reputation Risk
Risks
Regulatory Risk
Strategic Risk
Financial Risk
Data Privacy Risk

- Reputation Risk: The damage that can occur to a business when it fails to meet the expectations of its stakeholders and is thus negatively perceived with customers
- Strategic Risk: The risks of failing to achieve the business objectives and outcomes
- **Data Privacy Risk**: The potential loss of control over any personal/sensitive information during the engagement
- Financial Risk: The threat that hampers financial growth and company's profitability
- **Regulatory Risk:** Leading to non-compliance to meet laws, regulatory expectations
- Operational risk: The risk of losses caused by flawed or failed processes, policies, systems or events that disrupt business operations and resiliency
- **Technology Risk:** Any potential for technology failures to disrupt our business such as information security incidents, service outages, stability and availability

Third Party Vendor Categorization

Vendor categorization based on their exposure to data:

- High - *Vendors who have access to organization/customer data which consists of sensitive/personal/financial information and have a high risk of information loss (e.g. elancer, CNX)*

- Medium - *Vendors whose access to organization/customer data is limited (do not have access to sensitive/personal/financial customer information) (e.g. VVDN, Yantra)*

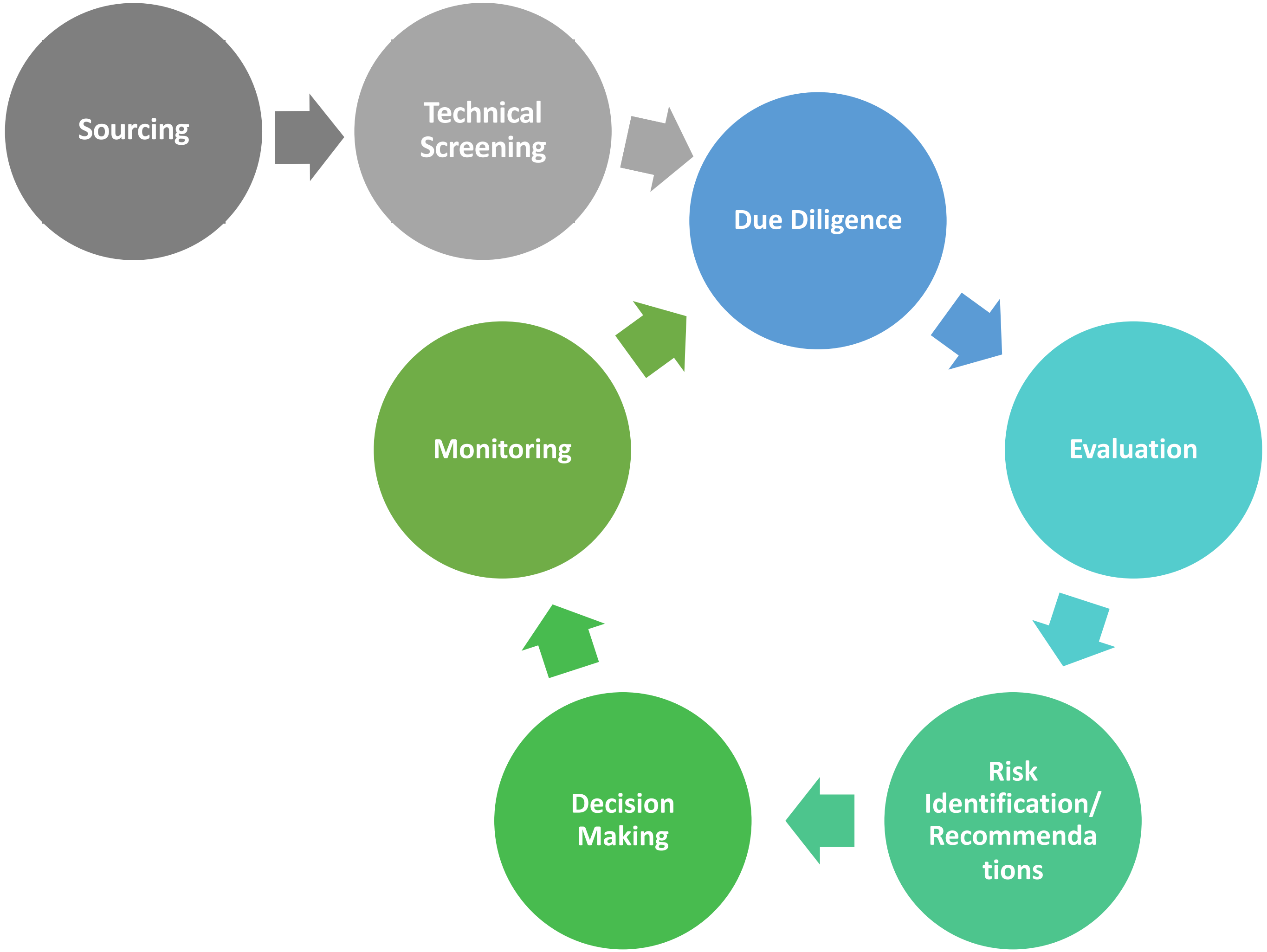
- Low - *Vendor who do not have access to organization/customer data (e.g. Microsoft)*

- Contractors/Consultants – *Temporary / Contingent resources who will have access to Netradyne systems*

TPRM to be performed on high and medium category vendors netradyne

TPRM Approach

TPRM to be performed on high and medium category vendors



- **Sourcing** - process of identifying the vendors who provide services/solutions (Requestor+ IT)
- **Technical Screening** - selection of vendors from sourcing list post initial discussion, fitment of products/services (Requestor, IT, Legal, HR)
- **Due Diligence-** initiation of assessment to analyze vendor capabilities to deliver the work with required set of procedures (InfoSec, Requestor, Vendor, Legal/IT)
- **Evaluation-** completing the assessment (Requestor, Infosec, Legal, IT)
- **Risk Identification/Recommendation-** if any risks identified, will check for implementation of controls to mitigate the risk (InfoSec)
- **Decision Making-** based on the outcome, infosec to recommend to go, no-go (InfoSec, Requestor, Legal, Finance)
- **Continuous Monitoring-** to maintain visibility of security controls(InfoSec, IT, Legal)

Infosec Governance Checkpoints

- Why is this vendor chosen?
- What is business requirement?
- What is the duration of this engagement?
- What is the vendor's reputation?
- What data will the vendor access to?
- Who can access the data?
- Where will the data be stored?
- How will our data be protected?
- How and when will our data be destroyed?
- What is the vendor’s Business Continuity/Disaster Recovery Plan?
- What is the vendor's security training process?
- How does the vendor vet sub-vendors?

*For Details refer to the Due Diligence, onboarding, and offboarding checklist: Checklist

THANK YOU