Integrating Data Analytics within a Third-Party Risk Management (TPRM) Program

By Catherine Tibaaga

Table of Contents

Purpose of the Presentation

- What is the objective of the presentation
  - The objective of the presentation is to
  - What is the Third-Party Risk Management Process?
- Data Analytics
  - What is Data Analytics?
  - Why is Data Analytics important in Third-Party Risk Management?
- How to Implement Data Analytics into Third-Party Risk Management?
  - Building and maintaining an inherent risk register
  - Building and maintaining a residual risk register
- Using the inherent and residual risk registers to create risk appetite
- Tools that support Third-Party Risk Analytics
- Conclusion

What is Third-Party Risk Management (TPRM)?

What is Risk?

- Risk is defined as the probability or likelihood that an event will lead to losses or produce adverse effects.

What is Risk Management?

- Risk management is the process of controlling and managing the events that could lead to losses or produce adverse effects.

What is Third-Party Risk?

- Third-party risk is the probability or likelihood that the use of a third-party (i.e. vendor or supplier) will lead to losses or produce adverse effects.
    - *Third-Party Inherent Risks:*The probability or likelihood of loss due to outsourcing to a third-party without taking into consideration compensating controls that they have in place. *They represent risks intrinsic to the function or process being outsourced.*

    - *Third-Party Residual Risk*: The probability or likelihood of loss due to outsourcing to a third-party after evaluating the compensating controls that they have in place.

- **What is Third-Party Risk Management (TPRM)?**
    - Third-party risk management is the process of controlling and managing activities associated with outsourcing that could lead to losses or produce adverse effects.

What is the TPRM Process?

Note: Third-Party Risk Management process is based on ISO 31000 guideline for Risk Management

What is the third-party risk management process?

- *Identify the inherent risks using the inherent risk questionnaire*
  - Work with the third-party relationship manager (1st line of defense) to complete the inherent risk questionnaire.
  - The inherent risk questionnaire should produce an inherent risk score for the outsourced function/process.
  - Refer to the Sample Risk Identification Questionnaire.
  - Leverage any Risk and Controls Self-Assessments performed on the function/process that is being outsourced to complete the inherent risk questionnaire.

- *Determine preliminary residual risk utilizing a due diligence questionnaire (DDQ) that is sent to the third-parties.*
  - Work with the third-party (vendor/supplier) to complete the preliminary DDQ.
  - The preliminary DDQ should produce a preliminary residual risk score which determines the level of risk associated with utilizing a third-party taking into consideration specific controls they have in place.
  - The preliminary residual risk score represents the residual risk associated with the third-party prior to sending any third-party risk assessments.
  - Refer to the Sample Preliminary Due Diligence Questionnaire.

- *Determine the type of risk assessments that need to be sent to the third-party based on the inherent and preliminary residual risk scores.*
  - The inherent risk score determines the type of risk assessments required since it represents the level of criticality associated with outsourcing a specific function or process.
  - The preliminary residual risk score should be taken into consideration as it will determine how to tailor the third-party risk

Third-Party Risk Management (TPRM) Process Cont.

- *Send the risk assessments to the third-party to complete with a list of documentation that the third-party can provide to support responses provided in the questionnaire.* Refer to the document checklist.
  - Risk assessments should include the following (Information Security, Business/Disaster Recovery, Financial, and Compliance).
  - Risk assessments should be tailored according to inherent and preliminary residual risk scores.
  - Third-party should return completed risk assessments with supporting documentation to TPRM.

  Evaluate third-party risk assessments to determine residual risk associated with third-parties.
  - TPRM should perform first-level review to ensure risk assessments are completed correctly and third-party sent back correct supporting documentation.
  - After first-level review, send risk assessments to the respective risk subject-matter experts (SMEs) for second-level review.
  - Risk SMEs should utilize documentation provided by third-party to support evaluations.
  - Risk SMEs should provide a Risk Summary Report with a Risk Mitigation Action Plan (R-MAP) to the business unit, line or department relationship manager (1st line of defense) that plans utilize the third-party.

- *Work with relationship manager and third-party to mitigate residual risks found during third-party risk assessment evaluation.*
  - Review the Risk Summary Report with the R-MAP with all parties.
  - Work with third-party to determine which risks can be mitigated. The third-party should commit to remediating high risks in 90 days, medium risks in 180 days and low risks in 365.

Third-Party Risk Management (TPRM) Process Cont.

- *Work with relationship manager and third-party to mitigate residual risks found during third-party risk assessment evaluation.*
  - Work with the third-party relationship manager and procurement to ensure that correct language regarding TPRM is included in the the contracts. Contract language should include information security, business continuity, disaster recovery,financial and compliance standards.
  - For correct contract language, refer to OCC 2013-29.
  - For risks that cannot be mitigated, TPRM should work with third-party relationship manager to undergo a risk acceptance process or choose an alternative third-party.
  - Risk acceptance process should be determined and approved by Enterprise/Operational Risk.

- *Monitor all residual risks found during the third-party risk assessment process using a residual risk register.*
  - Residual risk register should capture whether risks were accepted, mitigated or are in the process of being mitigated.
  - Similar to the residual risk register should be utilized to perform data analytics to determine risk trends for decision-making purposes. Refer to sample residual risk register.
  - Provide reporting to enterprise/operational risk and senior management on inherent and residual risk trends.
  - Hold monthly and quarterly meetings with departmental executives that utilize third-parties and enterprise/operational risk management to discuss reporting.

Integrating Data Analytics into Third-Party Risk Management

- To integrate data analytics into third-party risk management, TPRM programs should track specific data using inherent risk registers and residual risk registers throughout the entire TPRM process.
- Inherent risk registers track data that define the risks intrinsic to utilizing the third party without assessing third-party controls to manage and control risks. Refer to sample inherent risk register.
- Residual risk registers track data that define risks identified during third-party risk assessments. They include data on risks after evaluaing the effectiveness and maturity of third-party controls to prevent risks.
- By tracking inherent and residual risks, TPRM programs can perform data analysis to find risk trends that help the organization understand its third-party risk exposure.
- Data analysis is the process of collecting, reviewing, transforming and modeling data for the purposes of finding and communicating useful trends that enable decision-making.
- Through data analysis, TPRM programs can create reports that allow them to communicate with the other risk lines of defense to determine the risk appetite for third-parties.

Integrating Data Analytics into TPRM: Inherent Risk Register

- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the inherent risk register.
  - **Data Classification**
    - What percentage of third-parties have a data classification of PII or PHI
    - What percentage of third-parties have a data classification of highly confidential information?
    - What percentage of third-parties have a data classification of confidential information?
    - What percentage of third-parties have a data classification of public information?

  - **Inherent Risk Score**
    - What percentage of third-parties have a risk score of tier 1 (Critical third-parties)?
    - What percentage of third-parties have a risk score of tier 2?
    - What percentage of third-parties have a risk score of tier 3?
    - What percentage of third-parties have a risk score of tier 4?

  - **Connection between inherent risk score and data classification?**
    - The higher the data classification, the greater probability that the inherent risk score will be higher. For example, an outsourced function/process that handles PII or PHI may have a higher inherent risk score (i.e. tier 1) which means more due diligence is needed in the form of a third-party risk assessments.

**Critical third-parties represent vendors or suppliers that support core business functions. In the event they cannot meet their contractual obligations and/or service level agreements (SLAs), there exists the possibility of financial or reputational losses for the organization.*

Integrating Data Analytics into TPRM: Inherent Risk Register

- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the inherent risk register.
  - **First Lines of Defense: Business Units/Lines/Departments**
    - Which business units/lines/departments outsource the most?
      - Business units/lines/departments that outsource the most to third-parties expose the organization to more third-party risk.

    - Which business units/line/departments outsource more functions/processes with PII or PHI the most?
      - Business units/lines/departments that outsource outsource more functions with PII or PHI than other business units/lines/departments expose the organization to more privacy, information security, compliance and possibly financial risk if a data breach occurred.

  - **Business Continuity**
    - Which business units/lines/departments have business processes with a Recovery Time Objective (RTO) of 24 hours versus 48 hours versus 72 hours versus one week versus 30 days?
      - RTO represents the amount of time necessary for the third-party to resume business after a business interruption (i.e. data breach, natural disaster, human disaster).

      - An RTO <= 24 hours is more critical and the inherent risk score may be higher than third-parties with RTOs of 48, 27, one week or 30 days.

Using Data Analytics to Determine Third-Party Risk Appetite

- When performing data analysis on residual risks using the residual risk register, it is important that the data analysis capture the following information in reporting
  - What percentage of risks have been accepted, mitigated, or are in the process of being mitigated
  - What percentage of risks are overdue for mitigation
    - High: 90 days
    - Medium: 180 days
    - Low: 365 days
  - Which risk area has the most risks identified
  - Which risk area has identified the most high risks

- Once the

Thank You