



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

By Catherine Tibaaga

## Table of Contents



- What is the Third-Party Risk Management (TPRM)?
- What is the TPRM Process?
- Integrating Data Analytics into TPRM
- Integrating Data Analytics into TPRM: Inherent Risk Register
- Integrating Data Analytics into TPRM: Residual Risk Register
- Using Data Analytics for Third-Party Risk Appetite Purposes
- 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 outsourcing functions or processes to third-parties such as vendors and suppliers will lead to losses or produce adverse effects.
  - *Third-Party Inherent Risk:* The probability or likelihood of loss due to outsourcing functions or processes to third-parties without taking into consideration their compensating controls to prevent and control events that could lead to losses and adverse effects. *It is intrinsic to the function or process being outsourced.*
  - *Third-Party Residual Risk:* The probability or likelihood of loss due to outsourcing functions or processes to third-parties after evaluating their compensating controls to prevent and control events that could lead to losses and adverse effects.
- **What is Third-Party Risk Management (TPRM)?**
  - Third-party risk management is the process of controlling and managing activities associated with outsourcing functions or processes 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 Inherent Risk Questionnaire](http://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).
  - Leverage any Risk and Controls Self-Assessments (RCSAs) performed on the function/process prior to outsourcing to complete the inherent risk questionnaire.
  - Document all inherent risk scores in the inherent risk register. Refer to the [Sample Inherent Risk Register](http://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).
  
- *Determine preliminary residual risk utilizing the preliminary due diligence questionnaire (DDQ).*
  - 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 residual risk associated with utilizing a third-party.
  - The preliminary residual risk score also determines whether utilizing the third-party to support the outsourced function/process is within the third-party risk appetite for the organization. Refer to the [Sample Preliminary Due Diligence Questionnaire](http://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).


# What is the TPRM Process?



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

- *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 assessment based on the information provided from the third-party.
  - TPRM should send the following risk assessments to the third-party (*Information Security and Business Continuity/Disaster Recovery*).
  - TPRM should complete the following risk assessments internally (Financial, Compliance, and Reputational).
    - Financial Risk Assessments are completed utilizing three years of financial statements submitted by the third-party.
    - Compliance Risk Assessments can include an OFAC scan to ensure compliance with AML regulations.
    - Reputational Risk Assessments are completed utilizing Google Search or reputational risk tool (*Dun and Bradstreet, Lexis Nexis*)
  
- *Send the third-party risk assessments to the third-party to complete with a list of supporting documentation that the third-party can provide to support responses provided in the risk assessments.*
  - Risk assessments should include the following risk assessments from the following risk areas: Information Security, Business/Disaster Recovery, Financial, Reputational, and Compliance.
  - Risk assessments should be tailored according to inherent and preliminary residual risk scores.
  - The third-party should return completed risk assessments with supporting documentation to TPRM.

## What is the TPRM Process?

- 
- *Evaluate third-party risk assessments to determine residual risks associated with third-parties.*
    - TPRM should perform first-level review to ensure third-party risk assessments are completed correctly and that the third-party sent the correct supporting documentation.
    - After the first-level review, TPRM should send risk assessments to the respective risk subject-matter experts (SMEs) for the second-level review.
    - Risk SMEs should utilize supporting documentation provided by third-party to support their evaluations.
    - Risk SMEs should provide a Risk Mitigation Action Plan (R-MAP) to the third-party relationship manager (1st line of defense) and third-party.
    - Refer to the [Sample R-MAP](http://www.catherinetibaaga.com/resources) Template at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).
  - *Work with relationship manager and third-party to mitigate residual risks found during the third-party risk assessment evaluation.*
    - Review the the R-MAP with the third-party relationship manager and third-party.
    - 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 days.

## What is the TPRM Process?

- *Work with the relationship manager and the third-party to mitigate residual risks found during the third-party risk assessment evaluation.*
  - Work with the third-party relationship manager and procurement to ensure that the correct language regarding TPRM is included in 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 inherent risk register, 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](#) at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).
  - 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 (TPRM)



- 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 third-parties without assessing third-party controls to prevent risks. Inherent risk registers leverage information provided from the inherent risk questionnaire. Please refer to [Sample Inherent Risk Register](https://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](https://www.catherinetibaaga.com/resources).
- Residual risk registers track data that define risks identified during third-party risk assessments. They include data on risks after evaluating the effectiveness and maturity of third-party controls to prevent and mitigate risks. Please refer to [Sample Residual Risk Register](https://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](https://www.catherinetibaaga.com/resources).
- 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 to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - **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 severe 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 to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - **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 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  $\leq$  24 hours is more critical and the inherent risk score may be higher than third-parties with RTOs of 48, 72, one week or 30 days.

# Integrating Data Analytics into TPRM: Residual Risk Register

- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the residual risk register to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - How many identified residual risks represent each risk area?
  - What percentage of identified residual risks represent each risk area?
  - For each risk area, how many identified residual risks are high low, and medium?
  - For each risk area, what percentage of identified residual risks are high, low and medium?
  - For each risk area, how many high, medium, and low risks remain unmitigated but are within their 90, 180, 365-day deadlines respectively?
    - High Risks- 90 days maximum to mitigate
    - Medium risks- 180 days maximum to mitigate
    - Low Risks- 365 days maximum to mitigate
  - For each risk area, how many high, medium, and low risks remain unmitigated but are past the mitigation deadline?
    - Unmitigated risks that are past their mitigation deadlines (High- 90 days, Medium- 180 days, Low- 365 days) expose the organization to third-party risk.

## Note

\* Risk areas include information security, business continuity, disaster recovery, compliance, financial, and reputation.

\*Include the relationship owners and executives in the reporting.

# Integrating Data Analytics into TPRM: Residual Risk Register



- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the residual risk register to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - For each risk area, how many high, medium, and low risks have been accepted vs. mitigated?
  - For each risk area, how many high, medium, and low risks have been mitigated?
  - For each risk area, what percentage of high, medium, and low risks remain unmitigated but are within their 90, 180, 365-day deadlines respectively?
  - For each risk area, what percentage of high, medium, and low risks remain unmitigated but are past the mitigation deadline?
  - For each risk area, what percentage of high, medium, and low risks have been accepted vs. mitigated?
  - For each risk area, what percentage of high, medium, and low risks have been mitigated?

## Note

*\* Risk areas include information security, business continuity, disaster recovery, compliance, financial, and reputation.*

*\*Include the relationship owners and executives in the reporting.*

# Integrating Data Analytics into TPRM: Residual Risk Register

- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the residual risk register to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - **Business Units/Lines/Departments with Function/Processes**
    - **Unmitigated Risks**
      - For each risk area, which business units/lines/departments have the most high, medium and low risks that are unmitigated but are within their mitigation deadlines?
      - For each risk area, which business units/lines/departments have the most high, medium and low risks that are unmitigated and are past their mitigation deadlines?
      - For each risk area, which functions/processes have the most high, medium and low risks that are unmitigated but are within their mitigation deadlines?
      - For each risk area, which functions/processes have the most high, medium and low risks that are unmitigated and are past their mitigation deadlines?

## Note

\* Risk areas include information security, business continuity, disaster recovery, compliance, financial, and reputation.

\*Include the relationship owners and executives in the reporting.

# Integrating Data Analytics into TPRM: Residual Risk Register

- When creating reports for senior management, data reporting analysts should ensure that reports answer the following questions below when leveraging the residual risk register to perform data analysis. *The questions below do not represent all of the possible questions necessary to produce reports.*
  - **Business Units/Lines/Departments with Functions/Processes**
    - **Accepted Risks**
      - For each risk area, which business units/lines/departments have the most accepted high, medium and low risks?
      - For each risk area, which functions/processes have the most accepted high, medium, and low risks?
    - **Mitigated Risks**
      - For each risk area, which business units/lines/departments have the most mitigated high, medium, and low risks?
      - For each risk area, which functions/processes have the most mitigated high, medium and low risks?

## Note

*\* Risk areas include information security business continuity, disaster recovery, compliance, financial, and reputation.*

*\*Include the relationship owners and executives in the reporting.*

## Using Data Analytics for Third-Party Risk Appetite Purposes

- Once data analysis and reporting are completed, TPRM should use the risk trends identified in the reporting to determine the organization's risk exposure due to outsourcing functions or processes.
- The risk exposure should help the organization determine if third-parties utilized are within the organization's risk appetite for outsourcing.
- Risk appetite represents the amount of risk the organization wishes to absorb and tolerate. The risk appetite for the organization should be in alignment with corporate, industry and regulatory standards for the following risk areas below:
  - Information Security
  - Business Continuity/Disaster Recovery
  - Compliance
  - Financial and Reputational
- To determine if a third-party fits within the TPRM risk appetite, TPRM should utilize the questions in the preliminary DDQ and assign each question a weighted score. TPRM should work with the risk SMEs for each risk area to assign the correct score to each question. Please refer to the [Sample Preliminary DDQ](http://www.catherinetibaaga.com/resources) at [www.catherinetibaaga.com/resources](http://www.catherinetibaaga.com/resources).
- Each question in the preliminary DDQ reflects corporate, industry and regulatory standards for each risk area (i.e. information security, business continuity, disaster recovery, financial, compliance, and reputational).
- To produce a preliminary residual risk score, the third-party should complete the preliminary DDQ and the preliminary DDQ should assign a score based on the responses provided by the third-party.

## Using Data Analytics for Third-Party Risk Appetite Purposes

- The preliminary residual risk score should be based on a preliminary residual risk scoring scheme that is determined and approved by TPRM, the risk SMEs, Enterprise Risk/Operational Risk. It should be automated within the preliminary DDQ.
- The preliminary residual risk scoring scheme represents the third-party risk appetite for the organization. Please refer to the example below.

Residual Risk Score	Residual Risk Classification	Inside or Outside TPRM Risk Appetite	Action Required
25-30	Very Low	Inside	Move forward with TPRM process.
21-25	Low	Inside	Move forward with TPRM process.
16-20	Medium	Inside	Move forward with TPRM process.
6-15	High	Outside	Find an alternative third-party or ask for independent attestation. If independent attestation exists, move forward with TPRM process.
0-5	Very High	Outside	Do not utilize third-party. Find an alternative third-party.

- All residual risk scores should be recorded in the residual risk register. When performing data analysis, TPRM should determine the percentage of third-parties within the third-party population that fit within the defined third-party risk appetite as defined by the residual risk scoring scheme utilized in the preliminary DDQ.



# Conclusion

- Overall, data analytics enables TPRM programs to depict the risk trends associated with their third-party population.
- By incorporating data analytics into the TPRM process, it enables TPRM programs to quantify risk trends that define the third-party population.
- Quantifying risk trends allows an organization to fully understand their risk exposure and determine the level of action needed to control and mitigate risks that threaten the strategic objectives of the organization.
- Data analytics also enables TPRM programs to create their third-party risk appetite framework and determine if their third-party population is within the risk appetite for outsourcing.
- By understanding the risk appetite for the third-party population, the organization can proactively decide how to minimize the risks associated with outsourcing functions or processes while maximizing the benefits.



# Thank You



For more information, please contact Catherine Tibaaga

[info@catherinetibaaga.com](mailto:info@catherinetibaaga.com)

[www.catherinetibaaga.com](http://www.catherinetibaaga.com)

LinkedIn: [Catherine Tibaaga](#)