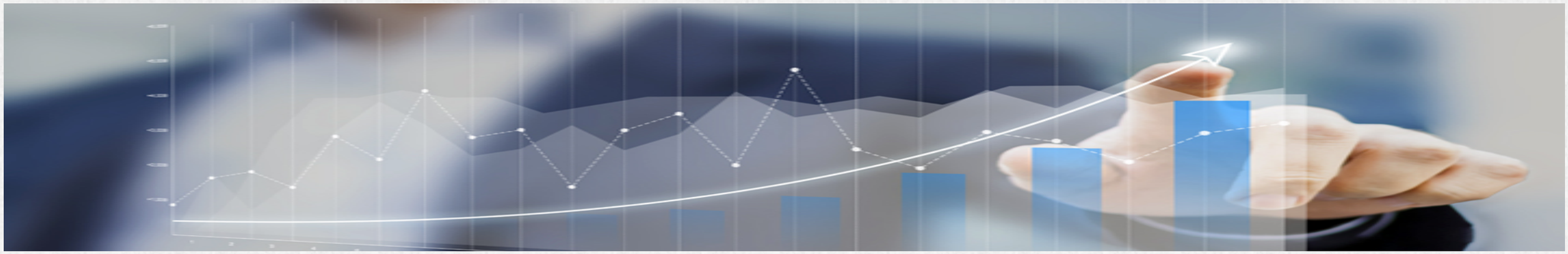
# Beginner’s Guide to Vendor, Supplier and Third-Party Risk Management

**By: Catherine Tibaaga**



# Table of Contents

# Objectives and Learning Outcomes

**-Objectives and Learning Outcomes**

- Understanding the importance of vendor, supplier and third-party risk management
- Building and maintaining vendor, supplier and third-party risk management programs
- Integrating vendor, supplier and third-party risk management into the vendor life cycle

**-Target Audience: Executives, managers, analysts and associates in financial services and healthcare that are responsible for the following tasks and duties listed below:**

- Vendor, supplier and third-party relationship managers responsible for managing the vendor, supplier, third-party risk management process
- Senior Management responsible for enterprise and/or operational risk management
- Legal and procurement professionals responsible for executing and negotiating contracts and agreements with vendors, suppliers and third-parties
- Risk subject-matter experts responsible for conducting third-party risk assessments (i.e. information security, business continuity, disaster recovery, compliance, and financial viability)

# Defining Vendor, Supplier or Third-Party Risk Management

**-What is Risk?**

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

- *Vendor, Supplier or Third-Party Inherent Risks*- Risks associated with outsourcing to a vendor, supplier or third-party without taking into consideration compensating controls that are in place to protect the organization. *They represent risks intrinsic to the function or process being outsourced without taking into consideration any controls implemented by the vendor, supplier or third-party.*
- *Vendor, Supplier or Third-Party Residual Risk*- Risks associated with outsourcing to a vendor, supplier or third-party after evaluating the compensating controls that are in place.

**-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 Vendor, Supplier or Third-Party Risk?**

Vendor, supplier or third-party risk is the probability or likelihood that the use of a vendor, supplier and/or third-party will lead to losses or produce adverse effects.

**-What is Vendor or Third-Party Risk Management?**

Vendor, supplier or third-party risk management is the process of controlling and managing activities associated with outsourcing that could lead to losses or produce adverse effects.

# The Importance of Vendor, Supplier or Third-Party Risk Management: Regulations, Benefits and Protection

## ***Regulations***

- Due to greater regulatory standards, many organizations such as financial institutions and healthcare organizations are required to perform due diligence on their vendors, suppliers and third-parties.
    - Examples: Office of the Comptroller (OCC), Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), Healthcare Insurance Portability Accountability Act (HIPAA).
- To meet regulatory demands, organizations should implement vendor, supplier or third-party risk management programs to ensure that they are maximizing the benefits of utilizing vendors, suppliers and third-parties and minimizing the risks.

## ***Benefits***

- *Reduce Costs and Improve Efficiency:* The use of vendors, suppliers or third-parties allows organizations to reduce their costs, to gain competitive advantage in their respective markets by engaging vendors, suppliers or third-parties.

## ***Protection***

- Despite the advantages associated with utilizing vendors, suppliers or third-parties, there exist various risks that could potentially undermine the goals and objectives of an organization.
- It is important to implement a vendor, supplier or third-party risk management process so that an organization is not adversely affected by the risks associated with their vendors, suppliers or third-parties.

# What are the Main Risks associated with Vendors, Suppliers or Third-Parties?

- **Enterprise Risk Management:** The probability or likelihood that specific events will have a positive or negative impact on an organization's ability to earn income and capital.
- **Operational Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party's inadequate processes, procedures, systems or people.
- **Financial Risk:** The probability or likelihood of material losses due to a company unable to earn adequate income, pay its debts and reward its shareholders.
- **Reputational Risk:** The probability or likelihood of material losses due to a company unable to earn adequate income, pay its debts and reward its shareholders.
- **Strategic Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party providing services or products that are not in alignment with an organization's business objectives. Business objectives may include improving profitability by increasing efficiency in processes to lower the costs of doing business.
- **Information Security Risk:** The probability or likelihood of material losses as a result of a vendor, supplier or third-party lacking adequate controls to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- **Business Continuity Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party lacking the controls in place to ensure that they can continue to provide services/products to the organization and meet their contractual Service Level Agreements (SLAs) in the event of a critical event.
- **Disaster Recovery Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party lacking the controls to ensure that vital technological systems, infrastructure and information is recoverable due to a natural and man-made disaster.
- **Contract and or Legal Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party not meeting their legal obligations as dictated by the contract to the organization.
- **Regulatory/Compliance Risk:** The probability or likelihood of material losses due to a vendor, supplier or third-party providing services or products that do not adhere to regulations, laws or industry standards.

## Who are the Various Stakeholders involved in the Vendor, Supplier or Third-Party Risk Management Process?

- **<u>Risk Subject-Matter Experts: Risk SMEs</u>**
  - **Information Security:** Ensures that vendor, supplier or third-party have adequate controls, policies and procedures in place to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. They ensure that the vendor, supplier or third-party controls maintain the confidentiality, integrity and availability of information.
  - **Business Continuity:** Ensures that the vendor, supplier or third-party have the controls in place to ensure that they can continue to provide services/products to the organization and meet their contractual Service Level Agreements (SLAs) in the event of a critical event.
  - **Disaster Recovery:** The probability or likelihood of material losses due to a vendor, supplier or third-party lacking the controls to ensure that vital technological systems, infrastructure and information are recoverable due to a natural or man-made disaster.
  - **Legal:** Creates the legal document that serves as a binding written contract between the vendor, supplier or third-party and the organization. The legal document contains any obligations that the vendor, supplier or third-party must meet from a regulatory, industry standard and operational risk perspective (i.e. indemnification, right-to-audit, insurance). May work in conjunction with ***procurement*** to draft and execute the contracts. May also work in conjunction with ***compliance*** to ensure that vendor, supplier or third-party contracts are written to reference appropriate regulations for the vendors, suppliers and third-parties to follow when providing products/services to the organization. Will also work with the other risk SMEs to ensure that best practices from various operational risk perspectives are incorporated into the contract (i.e. information security, business continuity standards).
  - **Compliance:** Ensures that vendor, supplier or third-party contracts are written to reference appropriate regulations for the vendor, supplier or third-party to follow when providing products/services to the organization. May also work in conjunction with legal**.**
  - **Finance:** Ensures that the vendor, supplier or third-party is able to meet its obligations to debtors and shareholders and can produce adequate income to continue to operate and provide products/services to its client/customer base.
  - **Insurance:** Ensures that the vendor, supplier or third-party has adequate protection from financial loss due to operational failure. May require the vendor, supplier or third-party to show proof of protection in the form of a certificate of insurance (COI) to determine if it is adequate to protect the organization from operational risk.

# Who are the Various Stakeholders Involved in the Vendor, Supplier and Third-Party Risk Management Process? (Continued)

- **1st Line of Defense: Business Units, Lines and Departments**
  - Vendor, Supplier or Third-Party Relationship Manager: Responsible for working with the risk SMEs to complete the vendor, supplier or third-party risk assessments. Utilizes the policies, processes and procedures as defined by the vendor, supplier or third-party risk management team in conjunction with the risk SMEs. Also performs the reputation risk assessment to determine if the vendor, supplier or third-party has a solid reputation that will not negatively impact the firm.

- **2nd Line of Defense: Vendor, Supplier or Third-Party Risk Management**
  - Vendor, Supplier or Third-Party Risk Management Group: Works with the other risk SME groups to create and implement the policies, processes and procedures that govern the vendor, supplier or third-party risk assessment process.

- **3rd Line of Defense: Auditors (Internal and External)**
  - **Internal Auditors:** A group within the organization that provides objective and independent assurance of the first, and second line of defense to ensure that vendor, supplier or third-party risk management is in alignment with industry best practices and regulations. They report back to Senior Management and the Board.
  - **External Auditors:** An entity outside the organization that provides objective and independent assurance of the first, and second line of defense to ensure that vendor, supplier or third-party risk management is in alignment with industry-best practices and regulations. They report back to Senior Management and the Board. They report back to Senior Management and the Board.

# What is the Vendor, Supplier or Third-Party Risk Assessment Process? (Identify, Assess, and Analyze)

*Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to complete the analysis portion of the vendor, supplier or third-party risk assessment.*

Identify inherent risks and potential residual risks

- The vendor, supplier or third-party relationship manager should identify risks intrinsic to the products/services being outsourced. Refer to the Sample Sample Risk Identification Questionnaire under Sample Risk Assessment Template.
- The vendor, supplier or third-party relationship manager should send a preliminary due diligence questionnaire the vendor, supplier or third-party. Refer to the Sample Preliminary Due Diligence Questionnaire.
- The vendor, supplier or third-party relationship manager should utilize processes, procedures and tools determined by vendor, supplier or third-party risk management (Second Line of Defense) to identify inherent risks and potential residual risks.
- Should be completed within the planning stage of the vendor, supplier or third-party life cycle as defined by procurement or sourcing.

Assess inherent and potential residual risks identified

- The vendor, supplier or third-party relationship manager should work with the vendor, supplier or third-party risk management and/or risk SMEs to verify the inherent and potential residual risks identified.
- Should be completed within the planning or due diligence stage of the vendor, supplier or third-party life cycle as defined by procurement or sourcing.

Analyze vendor, supplier or third-party controls

- Vendor, supplier or third-party relationship manager should send the vendor, supplier or third-party risk assessments to the vendor, supplier or third-party.
- The vendor, supplier or third-party should complete the vendor, supplier or third-party risk assessments and send them back to the vendor, supplier or third-party relationship manager.
- The vendor, supplier or third-party relationship manager should check to ensure all answers have been completed and that there do not exist any discrepancies in answers. If they exist, vendor, supplier or third-party relationship manager should check with vendor, supplier or third-party to correct any discrepancies prior to submitting to the risk SMEs.
- Send the fully completed vendor, supplier or third-party risk assessment to the risk SMEs to complete the analysis of the vendor's, supplier's or third-party's controls.
- The risk SMEs should provide their completed vendor, supplier or third-party risk assessment to the vendor, supplier or third-party relationship manager.
- Should be completed within the due diligence stage of the vendor, supplier or third-party life cycle as defined by corporate procurement or sourcing.

# What is the Vendor, Supplier or Third-Party Risk Assessment Process? (Mitigate and Monitor)

*Note: If an automated solution is utilized, the vendor, supplier or third-party relationship manager along with the vendor, supplier or third-party and risk SMEs should use the automated interface to complete the analysis portion of the vendor, supplier or third-party risk assessment.*

Mitigate the residual risks found during the vendor, supplier or third-party risk assessments

- The vendor, supplier or third-party relationship manager should discuss the findings along with recommended mitigation steps and dates with the vendor or third-party and risk SMEs.
- Using the recommended mitigation steps and dates, the vendor, supplier or third-party relationship manager should create a risk mitigation plan to submit to the vendor, supplier or third-party.
- The vendor, supplier or third-party relationship manager risk mitigation plan should be submitted to the vendor, supplier or third-party and the vendor, supplier or third-party risk management team (second line of defense) for mitigation and tracking purposes.
- Should be completed within the due diligence, implementation and monitoring stages of the vendor, supplier or third-party life cycle as defined by procurement or sourcing.

Monitor inherent and potential residual risks

*Note: Inherent and potential residual risks should be tracked separately.*

- The vendor, supplier or third-party relationship manager should work with the vendor, supplier or third-party risk management and/or risk SMEs to monitor the inherent and potential residual risks identified.
- Should be completed within the due diligence, implementation and monitoring stages of the vendor or third-party life cycle as defined by procurement or sourcing.

# Conclusion

- Risk exists in every aspect of operating a business.
- Despite the advantages of outsourcing, there exist risks that could potentially undermine an organization's strategic objectives.
- To control and mitigate risks associated with outsourcing, organizations should implement vendor, supplier or third-party risk management programs.
- By implementing a vendor, supplier or third-party risk management program, organizations can maintain a balance between risk and reward.
- Doing so enables the organization to maximize the benefits of outsourcing while minimizing the risks.

## Thank You


# Catherine Tibaaga

www.catherinetibaaga.com
info@catherinetibaaga.com